Libros de Cátedra

Notas de Álgebra y Matemática Discreta

Liliana Alcón

FACULTAD DE CIENCIAS EXACTAS

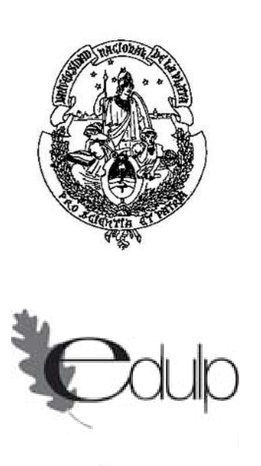






NOTAS DE ÁLGEBRA Y MATEMÁTICA DISCRETA

Liliana Alcón



2014

Alcón, Liliana

Notas de algebra y matemática discreta. - 1a ed. - La Plata : Universidad Nacional de La Plata, 2014.

E-Book: ISBN 978-950-34-1070-7

1. Álgebra. 2. Enseñanza Universitaria. I. Título

CDD 512.071 1

Fecha de catalogación: 08/04/2014

Diseño de tapa: Dirección de Comunicación Visual de la UNLP





Universidad Nacional de La Plata – Editorial de la Universidad de La Plata

47 N.º 380 / La Plata B1900AJP / Buenos Aires, Argentina
+54 221 427 3992 / 427 4898
editorial@editorial.unlp.edu.ar
www.editorial.unlp.edu.ar

Edulp integra la Red de Editoriales Universitarias Nacionales (REUN)

Primera edición, 2014
ISBN 978-950-34-1070-7

A quienes eligen estudiar.

Nota

El lector encontrará en este libro los temas comprendidos en la primera mitad del programa de la asignatura Álgebra que se dicta en la Facultad de Ciencias Exactas de la Universidad Nacional de La Plata para alumnos de las Licenciaturas en Matemática, Física, Astronomía y Geofísica, así como también para alumnos del Profesorado de Matemática. La profundidad con que son tratados los distintos puntos del temario y el orden en que se presentan están en concordancia con los requerimientos de dicha Cátedra.

Índice general

1. Lógica proposicional y teoría de conjuntos **1**

1.1. Elementos de lógica 1

1.1.1. Proposiciones, fórmulas proposicionales y tablas de verdad . . 1

1.1.2. Razonamientos 10

1.1.3. Funciones proposicionales, cuantificadores 14

1.2. Teoría de conjuntos 20

1.2.1. Definiciones básicas: subconjunto, conjunto vacío, complemento, conjunto de partes 20

1.2.2. Operaciones entre conjuntos 26

1.2.3. Familias de Conjuntos 31

2. Relaciones y Funciones **35**

2.0.4. Producto cartesiano y relaciones 35

2.0.5. Relaciones de orden 41

2.0.6. Relaciones de equivalencia 48

2.0.7. Funciones 51

2.0.8. Conjuntos coordinables 57

3. Números naturales. Conteo **61**

3.1. Propiedades de los números reales 61

3.2. Números naturales 65

3.2.1. Inducción y definiciones recursivas 65

3.2.2. Números Combinatorios y Binomio de Newton 76

3.3. Conteo 80

3.3.1. Ejemplos varios 89

4. Números enteros y números racionales **93**

4.1. Números enteros 93

4.1.1. Congruencias 111

4.2. Números racionales 115

5. Números complejos **121**

5.1. Forma de par ordenado. Operaciones. Forma binómica 121

5.2. Forma trigonométrica 128

5.3. Radicación de números complejos 134

5.3.1. Raíces n-ésimas de la unidad 136

6. Estructuras algebraicas **141**

6.1. Operaciones en un conjunto 141

6.1.1. Suma y producto en $\mathbb{Z}_n$ 145

6.2. Grupo. Anillo. Cuerpo 147

6.2.1. Subgrupo. Subanillo. Subcuerpo 150

7. Polinomios **157**

7.1. Suma y producto de polinomios. Propiedades 157

7.2. Divisibilidad en $\mathbb{K}[x]$ 162

7.3. Raíces de un polinomio 167

7.4. Polinomio derivado 172

Capítulo 1

Lógica proposicional y teoría de conjuntos

1.1. Elementos de lógica

1.1.1. Proposiciones, fórmulas proposicionales y tablas de verdad

Una **proposición** es una oración declamativa a la cual se le puede asignar un valor verdad: verdadera (V) o falsa (F). Las proposiciones serán simbolizadas mediantes letras minúsculas: p, q, r, etc.

Ejemplo 1.

Las siguientes oraciones son proposiciones:

5 es menor que 6.

$2 + 4 = 8$.

La suma de dos números reales positivos es un número real positivo. $\diamondsuit$

A partir de una o más proposiciones se pueden formar otras proposiciones utilizando los **operadores o conectivos lógicos**: conjunción, disyunción, condicional, bicondicional, y negación.

Conjunción: Si p y q son dos proposiciones cualesquiera, la conjunción de p y q es la proposición que se lee "p y q" y se simboliza $p \wedge q$. El valor de verdad de la proposición $p \wedge q$ está determinado por el valor de verdad de las proposiciones p y q según la siguiente tabla:

p	q	p $\wedge$ q
V	V	V
V	F	F
F	V	F
F	F	F

Ejemplo 2.

- De la conjunción de la proposición "5 es menor que 6" y la proposición "$2+4=8$" obtenemos la proposición "5 es menor que 6 y $2+4=8$". Como la proposición "5 es menor que 6" es verdadera y la proposición "$2+4=8$" es falsa, la proposición "5 es menor que 6 y $2+4=8$" es falsa.
- La proposición "$\sqrt{2}$ y $\sqrt{5}$ son números reales positivos" es la conjunción de la proposición "$\sqrt{2}$ es un número real positivo" y de la proposición "$\sqrt{5}$ es un número real positivo". Como la proposición "$\sqrt{2}$ es un número real positivo" es verdadera y la proposición "$\sqrt{5}$ es un número real positivo" también es verdadera, resulta que la proposición "$\sqrt{2}$ y $\sqrt{5}$ son números reales positivos" es verdadera. $\diamondsuit$

Disyunción: Si p y q son dos proposiciones cualesquiera, la disyunción de p y q es la proposición que se lee "p o q" y se simboliza $p \vee q$. El valor de verdad de la proposición $p \vee q$ está determinado por el valor de verdad de las proposiciones p y q según la siguiente tabla:

p	q	p $\vee$ q
V	V	V
V	F	V
F	V	V
F	F	F

Ejemplo 3.

De la disyunción de la proposición "5 es menor que 6" y la proposición "$2+4=8$" obtenemos la proposición "5 es menor que 6 o $2+4=8$". Como la proposición "5 es menor que 6" es verdadera y la proposición "$2+4=8$" es falsa, la proposición "5 es menor que 6 o $2+4=8$" es verdadera. $\diamondsuit$

Condicional: Si p y q son dos proposiciones cualesquiera, el condicional de p y q es la proposición que se lee "Si p entonces q" y se simboliza $p \to q$. El valor de verdad de la proposición $p \to q$ está determinado por el valor de verdad de las proposiciones p y q según la siguiente tabla:

p	q	p → q
V	V	V
V	F	F
F	V	V
F	F	V

En el condicional $p \to q$, la proposición p se llama **antecedente** y la proposición q se llama **consequente**. Existen otras formas de leer la proposición $p \to q$, a saber:

p implica q.
p sólo si q.
q es condición necesaria para p.
q si p.
p es condición suficiente para q.

Ejemplo 4.

- Como la proposición "5 es menor que 6" es verdadera y la proposición "$2+4=8$" es falsa, la proposición "Si 5 es menor que 6 entonces $2+4=8$" es falsa. Mientras que la proposición "Si $2+4=8$ entonces 5 es menor que 6" es verdadera.
- La proposición "Si 1 es negativo entonces -6 es positivo" es verdadera.
- La proposición condicional con antecedente "$\sqrt{2}$ es un número real" y consecuente "$1+3=4$" es la proposición "Si $\sqrt{2}$ es un número real entonces $1+3=4$".
- Las siguientes son formas equivalentes de decir una misma proposición,

  Si $8 \leq 6$ entonces $1+3=5$.
  $8 \leq 6$ implica $1+3=5$.
  $8 \leq 6$ sólo si $1+3=5$.
  $1+3=5$ es condición necesaria para que $8 \leq 6$.

$1+3=5$ si $8 \leq 6$.

$8 \leq 6$ es condición suficiente para $1+3=5$. ♢

Bicondicional: Si p y q son dos proposiciones cualesquiera, el bicondicional de p y q es la proposición que se lee "p si y sólo si q" y se simboliza $p \leftrightarrow q$. El valor de verdad de la proposición $p \leftrightarrow q$ está determinado por el valor de verdad de las proposiciones p y q según la siguiente tabla:

p	q	p ↔ q
V	V	V
V	F	F
F	V	F
F	F	V

Ejemplo 5.

- Como la proposición "5 es menor que 6" es verdadera y la proposición "$2+4=8$" es falsa, la proposición "5 es menor que 6 si y sólo si $2+4=8$" es falsa. Observar que la proposición "$2+4=8$ si y sólo si 5 es menor que 6" también es falsa.
- La proposición "1 es positivo si y sólo si -6 es negativo" es verdadera. ♢

Negación: Si p es una proposición cualquiera, la negación de p es la proposición que se lee "no p" y se simboliza $\sim p$. También puede decirse "es falso que p". El valor de verdad de la proposición $\sim p$ está determinado por el valor de verdad de las proposición p según la siguiente tabla:

p	∼ p
V	F
F	V

Ejemplo 6.

- Como la proposición "5 es menor que 6" es verdadera, la proposición "5 no es menor que 6" es falsa.
- La proposición "$3+5 \neq 9$" es la negación de la proposición "$3+5=9$".

- La proposición "es falso que 6 es un número real negativo" es la negación de la proposición "6 es un número real negativo". $\diamondsuit$

Se dice que la proposición

$q \to p$ es la implicación **recíproca** de $p \to q$;

$\sim p \to \sim q$ es la implicación **contraria** de $p \to q$;

$\sim q \to \sim p$ es la implicación **contrarecíproca** de $p \to q$.

Ejercicio 7.

1. Dadas las siguientes proposiciones:

   p: "$\mathbb{R}$ simboliza el conjunto de los números reales".

   q: "$3 + 1 = 7$".

   r: "3 es un número par".

   s: "la letra t es una vocal".

   t: "$\sqrt{2}$ es un número racional".

   a) Establecer el valor de verdad de cada una.

   b) Establecer el valor de verdad de las siguientes proposiciones e indicar como se leen en lenguaje corriente.

      1) $\sim q \wedge r$.

      2) $s \vee \sim t$.

      3) $\sim p \to \sim r$.

2. Determinar si las siguientes proposiciones son verdaderas o falsas:

   a) Si 9 es par entonces 3 es par.

   b) $2 + 2 = 4$ sólo si $2 + 2 = 3$.

   c) $1 + 1$ es 3 si $2 + 2$ es 4.

   d) 7 es par si 5 es par.

3. Reescribir las siguientes proposiciones utilizando "necesario" y "suficiente" y determinar su valor de verdad.

   a) $3 + 1 = 4$ sólo si $2 + 4 = 6$.

   b) $3 = 5$ si $3 = 7$.

c) $2-1=0$ si y sólo si $2+1=0$.

4. Dada la proposición: "*Si un número entero es múltiplo de* 4 *entonces es par*", enunciar los condicionales recíproco, contrario y contrarrecíproco y establecer el valor de verdad de cada uno de ellos. ♢

Una proposición obtenida a partir de otras proposiciones metiante el uso de conectivos lógicos se dice **compuesta**. Una proposición que no es compuesta se dice **atómica** o **simple**.

Ejemplo 8.

- "3 es menor que 5" es una proposición atómica.
- "Si $3+2=5$ y $5>8$, entonces $3+2<1$" es una proposición compuesta. Observa que como "$3+2=5$" es verdadera y "$5>8$" es falsa, "$3+2=5$ y $5>8$" es falsa. Resulta que la proposición "Si $3+2=5$ y $5>8$, entonces $3+2<1$" es verdadera. ♢

En la escritura corriente los signos de puntuación son utilizados para determinar el orden en que los conectivos actúan sobre distintas oraciones. Sin embargo, el uso de los mismos no siempre es claro y pueden producirse ambigüedades. Por ejemplo, llamemos p a la proposición atómica "$3+2=1$" (F), q a la proposición atómica "$6<7$" (V), y r a la proposición atómica "4 es positivo" (V).
La proposición que se lee "Es falso que $3+2=1$ o $6<7$ y 4 no es positivo", puede interpretarse de distintas maneras:

1. $\sim((p\vee q)\wedge\sim r)$. Como r es verdadera, $\sim r$ es falsa, y, en consecuencia, $(p\vee q)\wedge\sim r$ es falsa. Resulta que la proposición dada, $\sim((p\vee q)\wedge\sim r)$, es verdadera.
2. $(\sim p\vee q)\wedge\sim r$. Como r es V, $\sim r$ es F . Resulta que la proposición dada, $(\sim p\vee q)\wedge\sim r$, es falsa.

¿Cómo deberían intercalarse en el texto comas, dos puntos, etc. para que la oración adopte uno u otro significado?
Cuando es necesario para evitar estas ambigüedades, los enunciados matemáticos son simbolizados obteniendo fórmulas en las cuales el orden de conección entre las

partes que la componen está claramente determinado gracias al uso de paréntesis y las siguientes reglas:

Sea $\mathcal{P}$ el conjunto de todas las proposiciones. Una **variable proposicional** es un símbolo p, q, r, etc., que toma valores en $\mathcal{P}$. Las **fórmulas del cálculo proposicional**, que se indicanrán con letras mayúsculas, están definidas por las siguientes reglas:

1. Toda variable proposicional es una fórmula.
2. Si P es una fórmula entonces $\sim P$ es una fórmula.
3. Si P y Q son fórmulas entonces $(P \wedge Q)$, $(P \vee Q)$, $(P \to Q)$ y $(P \leftrightarrow Q)$ son fórmulas.
4. Siempre que se aplique una cantidad finita de veces cualquier combinación de las reglas anteriores se obtiene una fórmula.

Observación: es usual omitir la escritura de un juego de paréntesis que "encierra" toda una fórmula proposicional. También es usual decir "proposición" en lugar de "fórmula proposicional", aunque esto puede confundir a quienes están comenzando a estudiar el tema. Puede escribirses $P(p, q, ...)$ para indicar que la fórmula P depende de las variables p, q,....

Como en los casos más sencillos, usaremos tablas para analizar el valor de verdad de una proposición compuesta simbolizada mediante una determinada fórmula según sea el valor de verdad de las proposiciones atómicas que la compongan. Cada fila de la tabla corresponde a un valor de verdad de las proposiciones atómicas, resulta que si la fórmula depende de n variables entonces la tabla tendrá 2^n filas por debajo del encabezado.

Ejemplo 9.

Consideremos la fórmula $(\sim p \vee q) \to q$. Su tabla de verdad es

p	q	$\sim p$	$\sim p \vee q$	$(\sim p \vee q) \to q$
V	V	F	V	V
V	F	F	F	V
F	V	V	V	V
F	F	V	V	F

La tabla de verdad de la fórmula $(p\vee \sim r) \rightarrow ((p \wedge q) \vee r)$ es

p	q	r	$\sim r$	$p\vee \sim r$	$p \wedge q$	$(p \wedge q) \vee r$	$(p\vee \sim r) \rightarrow ((p \wedge q) \vee r)$
V	V	V	F	V	V	V	V
V	V	F	V	V	V	V	V
V	F	V	F	V	F	V	V
V	F	F	V	V	F	F	F
F	V	V	F	F	F	V	V
F	V	F	V	V	F	F	F
F	F	V	F	F	F	V	V
F	F	F	V	V	F	F	F

$\diamondsuit$

Ejercicio 10.

Calcular la tabla de verdad de cada una de las siguientes fórmulas:

1. $p \wedge \sim ((q \vee \sim r) \wedge s)$.
2. $(t \vee r) \rightarrow (q \wedge \sim r)$.
3. $((p\vee \sim q)\wedge \sim q) \rightarrow \sim p$.
4. $(((p \wedge q) \vee r) \vee q) \rightarrow \sim p$. 

Una **tautología** es una fórmula proposicional que siempre toma el valor de verdad Verdadero (V) independientemente del valor de verdad de las proposiciones atómicas que la componen; es decir, son aquellas fórmulas que en la ultima columna de su tabla de verdad presentan una "V" en cada fila. Por el contrario, cuando siempre toma el valor de verdad Falso (F), la fórmula se llama una **contradicción**.

Ejemplo 11.

Cada una de las siguientes fórmulas es una tautología: $p\vee \sim p$; $(p \wedge q) \rightarrow p$; $((p \wedge q) \vee (p\wedge \sim q))\vee \sim p$.

Las siguientes fórmulas son contradicciones: $p\wedge \sim p$; $p \leftrightarrow \sim p$. $\diamondsuit$

Dos fórmulas P y Q se dicen **lógicamente equivalentes** cuando dependen de las mismas proposiciones atómicas y tienen *la misma* tabla de verdad, esto significa que a igual valor de verdad de las proposiciones atómicas se obtiene igual valor de verdad para P que para Q. También podemos decir que P y Q son lógicamente equivalentes cuando $P \leftrightarrow Q$ es una tautología. Indicamos que P y Q son equivalentes escribiendo

$P \equiv Q$ o escribiendo $P \iff Q$. Utilizaremos proposiciones equivalentes para expresar una misma idea de distintas maneras.

Ejemplo 12.

Sea $P(p,q)$ la fórmula $p \to q$ y $Q(p,q)$ la fórmula $\sim p \vee q$. Sus tablas de verdad son *iguales*:

p	q	$p \to q$
V	V	V
V	F	F
F	V	V
F	F	V

p	q	$\sim p$	$\sim p \vee q$
V	V	F	V
V	F	F	F
F	V	V	V
F	F	V	V

Observar que la fórmula $P \leftrightarrow Q$, cuya expresión es $(p \to q) \leftrightarrow (\sim p \vee q)$, es una tautología dado que su tabla de verdad es

p	q	$p \to q$	$\sim p$	$\sim p \vee q$	$(p \to q) \leftrightarrow (\sim p \vee q)$
V	V	V	F	V	V
V	F	F	F	F	V
F	V	V	V	V	V
F	F	V	V	V	V

Entonces podemos escribir $(p \to q) \Leftrightarrow (\sim p \vee q)$, o bien, $(p \to q) \equiv (\sim p \vee q)$ y decir que $p \to q$ es lógicamente equivalente a $\sim p \vee q$. $\diamondsuit$

Ejercicio 13.

1. Probar las siguientes equivalencias lógicas.

   a) Doble Negación:

   - $p \iff \sim(\sim p)$

   b) Leyes Conmutativas:

   - $p \wedge q \iff q \wedge p$
   - $p \vee q \iff q \vee p$

   c) Leyes Distributivas:

   - $(p \vee q) \wedge r \iff (p \wedge r) \vee (q \wedge r)$
   - $(p \wedge q) \vee r \iff (p \vee r) \wedge (q \vee r)$

d) Leyes Asociativas:

- $p \wedge (q \wedge r) \iff (p \wedge q) \wedge r$
- $p \vee (q \vee r) \iff (p \vee q) \vee r$

e) Leyes de De Morgan:

1) $\sim (p \wedge q) \iff \sim p \vee \sim q$
2) $\sim (p \vee q) \iff \sim p \wedge \sim q$

2. Demostrar las siguientes equivalencias:

- $p \to q \iff (\sim q \to \sim p)$
- $p \to q \iff \sim p \vee q$
- $\sim (p \to q) \iff p \wedge \sim q$
- $p \leftrightarrow q \iff (p \to q) \wedge (q \to p)$ ♢

Convención: dada la propiedad asociativa de la conjunción y de la disyunción, con el objetivo de simplificar la notación, si P, Q y R son fórmulas cualesquiera, podemos escribir

$$P \wedge Q \wedge R \text{ en lugar de } (P \wedge Q) \wedge R, \text{ o en lugar de } P \wedge (Q \wedge R);$$

y podemos escribir

$$P \vee Q \vee R \text{ en lugar de } (P \vee Q) \vee R, \text{ o en lugar de } P \vee (Q \wedge R).$$

1.1.2. Razonamientos

Una propiedad distintiva del ser humano es el razonamiento: a partir de datos parciales se obtiene una conclusión, un nuevo conocimiento. Decimos que un **razonamiento** o **argumento** consta de un conjunto de proposiciones llamadas **premisas** y de una proposición llamada **conclusión**.

Consideremos el razonamiento

Premisa:	El estanque A está lleno o el estanque B está lleno
Premisa:	El estanque A está vacío
Conclusión:	El estanque B está lleno

y el razonamiento

Premisa:	El estanque A está lleno o el estanque B está lleno
Premisa:	El estanque A está lleno
Conclusión:	El estanque B está vacío

Intuitivamente vemos que el primer razonamiento es bueno, válido; en cambio, el segundo no lo es. Además, podemos entender que la validez de un razonamiento es independiente de las proposiciones particulares involucradas; por ejemplo, el primer razonamiento responde a la fórmula general:

$$\frac{\begin{array}{c} p \vee q \\ \sim p \end{array}}{q}$$

Todo razonamiento que pueda ser simbolizado de esta manera es válido.
Para indicar un razonamiento con premisas $P_1, P_2, ..., P_n$ y conclusión Q utilizaremos cualquiera de las dos notaciones siguientes:

$$P_1, P_2, ..., P_n \vdash Q \qquad \text{o} \qquad \frac{\begin{array}{c} P_1 \\ P_2 \\ \vdots \\ P_n \end{array}}{Q}$$

El razonamiento se dice **válido** cuando $(P_1 \wedge P_2 \wedge ... \wedge P_n) \to Q$ es una tautología. Observar que, efectivamente, la fórmula $((p \vee q) \wedge \sim p) \to q$ que corresponde al primer razonamiento es una tautología; en tanto, la fórmula $((p \vee q) \wedge p) \to \sim q$, que corresponde al segundo razonamiento, no lo es.

Un razonamiento que no es válido se dice una **falacia**.
Los siguientes son ejemplos de razonamientos válidos. Podría decirse que estos son razonamientos elementales, base de otros razonamientos más complejo.

1. $(p \wedge q) \vdash p$ (Simplificación)
2. $p, q \vdash (p \wedge q)$ (Adjunción)
3. $p \vdash (p \vee q)$ cualquiera sea q. (Adición)

4. $p,\ (p \to q) \vdash q$ (Modus Ponens)
5. $\sim q,\ (p \to q) \vdash \sim p$ (Modus Tollens)
6. $\sim p,\ (p \vee q) \vdash q$ (Silogismo disyuntivo)
7. $(p \to q),\ (q \to r) \vdash (p \to r)$ (Silogismo Hipotético)
8. $(p \vee p) \vdash p$
9. $(p \vee q),\ (p \to r),\ (q \to s) \vdash (r \vee s)$
10. $(p \vee q),\ (p \to r),\ (q \to r) \vdash r$

En general, para probar la validez de un razonamiento $P_1, P_2, ..., P_n \vdash Q$, podemos utilizar dos técnicas: 1) realizar la tabla de verdad para verificar que $(P_1 \wedge P_2 \wedge ... \wedge P_n) \to Q$ es una tautología; o 2) utilizar algunas de las premisas dadas como premisas de razonamientos válidos elementales (los indicados anteriormente); usar las conclusiones de estos razonamientos como premisas de nuevos razonamientos válidos elementales; así sucesivamente hasta obtener a Q como conclusión de uno de ellos.

Ejemplo 14.

Para probar la validez del razonamiento

$$\begin{array}{c} p \to q \\ \sim r \to \sim q \\ p \vee t \\ t \to s \\ \sim r \\ \hline s \end{array}$$

podemos:

1) verificar que la fórmula

$$(((((p \to q) \wedge (\sim r \to \sim q)) \wedge (p \vee t)) \wedge (t \to s)) \wedge \sim r) \to s$$

es una tautología realizando la correspondiente tabla de verdad.

2) utilizar las premisas dadas en razonamientos elementales válidos obteniendo conclusiones parciales. Éstas conclusiciones parciales son premisas de nuevos razonamientos válidos elementales.

$$\dfrac{\sim r \rightarrow \sim q \quad \sim r}{\sim q} \qquad \dfrac{p \rightarrow q \quad \sim q}{\sim p} \qquad \dfrac{p \vee t \quad \sim p}{t} \qquad \dfrac{t \rightarrow s \quad t}{s}$$

$\diamondsuit$

Ejercicio 15.

1. Analizar si los siguientes razonamientos son válidos.

(i) $p \rightarrow q$
$t \vee \sim q$
$s \wedge p$
———
$s \wedge \sim t$

(j) $p \leftrightarrow q$
$p \vee q$
———
$q \wedge \sim p$

(k) $\sim (p \wedge q)$
$\sim q \rightarrow t$
$\sim p \rightarrow t$
$s \rightarrow \sim t$
———
$\sim s$

(l) $p \rightarrow \sim q$
$\sim q \rightarrow \sim s$
$(p \rightarrow \sim q) \rightarrow \sim t$
$r \rightarrow t$
———
$\sim r$

2. Hallar los errores en las siguientes deducciones y corregirlos.

(1) $\sim t \vee \sim r$	Premisa
(2) $s \rightarrow (t \wedge r)$	Premisa
(3) $q \rightarrow s$	Premisa
(4) $q \vee p$	Premisa
(5) $\sim (t \wedge r)$	de (1) por Leyes de De Morgan
(6) $\sim s$	de (5),(2) y (3) por Modus Tollendo Ponens
(7) $\sim\sim q$	de (3) y (6) por Modus Tollens
(8) p	de (3) y (7) por Modus Tollendo Ponens

(1) $\sim s \rightarrow \sim t$	Premisa
(2) t	Premisa
(3) $s \rightarrow (r \wedge q)$	Premisa
(4) $(q \wedge r) \rightarrow p$	Premisa
(5) $\sim s$	de (1) y (2) por Modus Tollens
(6) s	de (5) por Doble Negación
(7) $r \wedge q$	de (3) y (6) por Modus Tollens
(8)p	de (5) y (7) por Modus Ponens

3. Simbolizar y decir si son válidos los siguientes razonamientos:

   a) Un sistema de riego con 5 estanques P, Q, R, S y T, interconectados, se rige por las siguientes reglas:

   Si el estanque Q tiene agua, el estanque P no la tiene. El estanque P tiene agua o el R está vacío. Si el estanque T tiene agua entonces el R tiene agua. El estanque S tiene agua o el estanque Q la tiene.

   Un operario observa que el estanque S no tiene agua y concluye que el estanque T no tiene agua.

   b) Un jóven le pregunta al profesor de lógica si aprobó el examen y el profesor le responde:

   Pedro es bueno, y Silvia es buena o Teresa es buena. Pedro es malo o Silvia no es buena. Teresa es mala o aprobaste el examen.

   El alumno piensa unos instantes y conluye: ¡aprobé el examen! ♢

1.1.3. Funciones proposicionales, cuantificadores

Sea x una variable que toma valores en un conjunto universal U. Una **función proposicional en la variable** x es una oración que depende de x de forma tal que al reemplazar x por cualquier elemento de U se obtiene una proposición. Las funciones proposicionales se indican $p(x)$, $q(x)$, etc; y los elementos del conjunto universal se llaman **constantes**.

Ejemplo 16.

La siguiente es una función proposicional dependiente de la variable x que toma valores en el conjunto $\mathbb{R}$ de los números reales.

$$p(x): \quad x + 10 > 0.$$

Es claro que "$x + 10 > 0$" no es una proposición: no puedo asignarle una valor de verdad pues depende de la variable x. ♢

Una función proposicional $p(x)$ se puede transformar en una proposición de tres formas disitintas:

1. reemplazando la variable por una constante;
2. anteponiendo el **cuantificador existencial** $\exists$,

   $$(\exists\, x)\, p(x)$$

   que se lee "existe x tal que $p(x)$ es verdadera" (o simplemente "existe x tal que $p(x)$");
3. anteponiendo el **cuantificador universal** $\forall$,

   $$(\forall\, x)\, p(x)$$

   que se lee "para todo x, $p(x)$ es verdadera" (o simplemente "para todo x, $p(x)$").

Ejemplo 17.

Continuando con el ejemplo anterior, haciendo $x = 1$ obtenemos la proposición $p(1)$:

$$1 + 10 > 0$$

que es verdadera. Haciendo $x = -20$ obtenemos la proposición $p(-20)$:

$$-20 + 10 > 0$$

que es falsa. Anteponiendo el cuantificador existencial obtenemos la proposición

$$(\exists\, x)\; x + 10 > 0$$

que es verdadera. Anteponiendo el cuantificador universal obtenemos la proposición

$$(\forall\, x)\, x + 10 > 0$$

que es falsa. ♢

La proposición $(\exists\, x)\, p(x)$ es verdadera cuando existe al menos un elemento del conjunto universal, llamémosle a, tal que $p(a)$ es verdadera. En este caso decimos que $p(x)$ es verdadera para *algún* elemento del conjunto universal.
En cambio, la proposición $(\forall\, x)\, p(x)$ es verdadera cuando $p(x)$ resulta una proposición verdadera al reemplazar x por *cualquier* elemento del conjunto universal. En otras palabras, esta proposición es falsa si existe algún elemento a del universal tal que $p(a)$ es falsa. En tal caso se dice que a es un **contraejemplo** de la proposición $(\forall\, x)\, p(x)$.
Si el uso de las palabras *algún* y *cualquier* resulta confuso, se puede pensar en ejemplos del lenguaje cotidiano:
Si digo "Algunos temas me interesan", se entiende que al menos hay un tema que es de mi interés. Mientras que si digo "Cualquier tema me interesa" se entiende que me interesan todos los temas.

Ejercicio 18.

1. Decidir cuáles de los siguientes enunciados son funiones proposicionales dependientes de una variable y definir un universo apropiado en cada caso.
   - "x es un número impar".
   - "$x - 3$ es múltiplo de 5".
   - "x es divisible por y".
2. Para las funciones proposicionales del ejercicio anterior, dar constantes que produzcan proposiciones verdaderas y proposiciones falsas.
3. Dadas las siguientes funciones proposicionales:
   - Si x es par entonces $x + 2$ es par.
   - $x + 5 \geq 20$ y $x - 6 \leq 22$.
   - $x - 1 > 1 \rightarrow x > 5$.

   a) Establecer un universo adecuado.
   b) Anteponer el cuantificador universal a cada uno de ellos, pasar al lenguaje corriente las proposiciones obtenidas y analizar su valor de verdad.
   c) Anteponer el cuantificador existencial a cada uno de ellos, pasar al lenguaje corriente las proposiciones obtenidas y analizar su valor de verdad.

d) Discutir la diferencia entre las siguientes proposiciones

$$(\forall x)(p(x) \to q) \quad \text{versus} \quad (\forall x)p(x) \to q$$
$$(\exists x)(p(x) \to q) \quad \text{versus} \quad (\exists x)p(x) \to q$$

$\diamondsuit$

Sea x una variable que toma valores en un conjunto U_x y consideremos otra variable y que toma valores en un conjunto U_y. Una oración que depende de estas dos variables de forma tal que al reemplazar x por un elemento cualquiera de U_x y reemplazar y por un elemento cualquiera de U_y se obtiene una proposición, se dice una **función proposicional en las variables** x **e** y. Usaremos la notación $p(x, y)$, $q(x, y)$, etc., para denotarlas.

Una función proposicional $p(x, y)$ se puede transformar en una proposición reemplazando las variables por constantes de sus respectivos conjuntos universales o anteponiendo dos cuantificadores:

1. $(\forall\, x)\, (\forall y)\, p(x, y)$
   que se lee "para todo x y para todo y, $p(x, y)$ es verdadera" .
2. $(\forall\, x)\, (\exists y)\, p(x, y)$
   que se lee "para todo x, existe y tal que $p(x, y)$ es verdadera" .
3. $(\exists\, x)\, (\forall y)\, p(x, y)$
   que se lee "existe x tal que, para todo y, $p(x, y)$ es verdadera" .
4. $(\exists\, x)\, (\exists y)\, p(x, y)$
   que se lee "existen x e y tales que $p(x, y)$ es verdadera" .

Ejemplo 19.

Sean x e y variables que toman valores en el conjunto de los números reales y sea la función proposicional $x \leq y$.

- $(\forall x)(\forall y)\ x \leq y$
  Dice que, dados dos números reales cualesquiera x e y, el primero es menor o igual que el segundo. Esta proposición es Falsa.
- $(\forall x)(\exists y)\ x \leq y$
  Dice que, dado un número real cualquiera x, es posible encontrar un número real y tal que x es menor o igual que y. Observar que el número y puede variar con x. Esta proposición es Verdadera.

- $(\exists x)(\forall y)\ x \leq y$

  Dice que existe un número real que es menor o igual que cualquier otro número real. Esta proposición es Falsa.
- $(\exists x)(\exists y)\ x \leq y$

  Dice que existe un par de números reales tal que el primero es menor que el segundo. Esta proposición es Verdadera.

Observar que cuando x e y son variables que toman valores en el conjunto de los números naturales, la primer proposición es falsa, en tanto que las tres restantes son verdaderas. $\diamondsuit$

Ejercicio 20.

1. Sea U_x el conjunto de alumnos regulares de Medicina y sea U_y el conjunto de materias del plan de estudio de dicha carrera. Llamemos $p(x, y)$ a la función proposicional "el alumno x ha aprobado la materia y", interprete en este caso el significado de cada una de las cuatro proposiciones que se obtienen al anteponer los cuantificadores $\exists$ y $\forall$.
2. Dadas las siguientes funciones proposicionales en las variables x e y que toman valores en el conjunto de los números naturales $\mathbb{N}$,

   - $N(x)$: x es par.
   - $I(x, y)$: x es igual a y.
   - $E(x)$: x es multiplo de 4.
   - $D(x, y)$: $x + y = 6$.
   - $M(x, y)$: x es mayor o igual que y.

   Pasar al lenguaje corriente:

   a) $(\forall x)(N(x) \to E(x))$
   b) $(\exists x)(E(x) \wedge (\sim N(x)))$
   c) $(\forall x)(\forall y)((N(x) \wedge N(y) \wedge D(x, y) \wedge D(y, x)) \to I(x, y))$
   d) $(\exists x)(\exists y)(E(x) \wedge E(y) \wedge D(x, y) \wedge D(y, x) \wedge \sim I(x, y))$
   e) $(\exists x)(N(x) \wedge M(x, 0))$
   f) $(\forall x)(E(x) \wedge M(0, x))$
   g) $\sim ((\forall x)(N(x) \wedge M(x, 0)))$
3. Simbolizar utilizando esquemas, cuantificadores y conectivos lógicos:

a) No todos los números enteros son positivos.

b) Dados dos números reales cualesquiera, si el primero es mayor que el segundo entonces el segundo es negativo.

c) Existe un número real tal que todo otro número mayor que él es positivo. ♢

Es claro que como $(\exists\, x)\, p(x)$ y $(\forall\, x)\, p(x)$ son proposiciones, ellas pueden ser vinculadas con otras proposiciones mediante conectivos lógicos o pueden formar parte de razonamientos, ya sea como premisas o como conclusión.

Ejemplo 21.

- Podemos simbolizar la proposición " Algunos números reales son racionales o todos los números reales son positivos" considerando una variable x que toma valores en el conjunto de los números reales $\mathbb{R}$ y dos funciones proposicionales:

  $p(x)$: x es racional.

  $q(x)$: $x > 0$.

  De esta forma la proposición dada se escribe

$$(\exists x)\, p(x) \;\vee\; (\forall x)\, q(x).$$

- Análogamente la proposición " Todos los números reales son no positivos implica algunos números reales son racionales" se simboliza

$$(\forall x) \;\sim q(x) \to (\exists x)\, p(x).$$

- Decir que es falso que una propiedad dada se cumple para todos los elementos de un conjunto universal, es claramente equivalente a decir que existe algún elemento del universal que no satisface dicha propiedad. Luego tenemos la equivalencia

$$\sim (\forall x) p(x) \;\;\equiv\;\; (\exists x) \sim p(x)$$

- Decir que es falso que una propiedad dada se cumple para algún elemento del universal, es claramente equivalente a decir que todos los elementos del universal no satisfacen dicha propiedad. Luego tenemos la equivalencia

$$\sim (\exists x) p(x) \;\;\equiv\;\; (\forall x) \sim p(x)$$

Ejemplo 22.

La negación de

$$(\exists x)(p(x) \vee (\forall y)h(y)) \leftrightarrow q$$

es

$$(\forall x)(\sim p(x) \wedge (\exists y) \sim h(y)) \leftrightarrow \sim q$$

pues

$$\begin{aligned} & \sim((\exists x)(p(x) \vee (\forall y)h(y)) \leftrightarrow q) && \equiv \\ \equiv \;& \sim((\exists x)(p(x) \vee (\forall y)h(y))) \leftrightarrow \sim q && \equiv \\ \equiv \;& (\forall x) \sim (p(x) \vee (\forall y)h(y)) \leftrightarrow \sim q && \equiv \\ \equiv \;& (\forall x)(\sim p(x) \wedge \sim (\forall y)h(y)) \leftrightarrow \sim q && \equiv \\ \equiv \;& (\forall x)(\sim p(x) \wedge (\exists y) \sim h(y)) \leftrightarrow \sim q \end{aligned}$$

♢

Ejercicio 23. Negar las proposiciones simbolizadas en el punto 2. del ejercicio 20 obteniendo una forma equivalente y expresarlas en lenguaje corriente. ♢

1.2. Teoría de conjuntos

1.2.1. Definiciones básicas: subconjunto, conjunto vacío, complemento, conjunto de partes

A lo largo de esta sección consideraremos un conjunto universal **U**. Sea x una variable que toma valores en **U** y sea $p(x)$ una función proposicional sobre x (digamos una propiedad enunciable sobre x).

Indicaremos con $\{x : p(x)\}$ al conjunto formado por los elementos del universal que satisfacen la propiedad $p(x)$, es decir, formado por los elementos a del universal tales que $p(a)$ es verdadera. Por simplicidad los conjuntos serán llamados con letras mayúsculas; diremos, por ejemplo,

sea C el conjunto $\{x : p(x)\}$; o bien,

sea $C = \{x : p(x)\}$.

Indicaremos que a es un elemento del conjunto C escribiendo $a \in C$; se lee "a **pertenece a** C". Observar que $a \in C$ significa que $p(a)$ es verdadera. La negación de

$a \in C$ se escribe $a \notin C$ y se se lee "a **no pertenece a** C".

Algunos conjuntos también puede ser definidos mediante la enumeración de sus elementos, en este caso se dice **definido por extensión**; mientras que, en el primer caso (utilizando una propiedad que caracteriza los elementos), se dice **definido por comprensión**.

Ejemplo 24.

Definiciones por comprensión:

$$A = \{x : x \text{ es un número natural menor que diez }\},$$

$$B = \{x : x \text{ es una vocal de la palabra matemática}\},$$

$$\mathbb{R} = \{x : x \text{ es un número real}\}.$$

Los conjuntos anteriores definidos por extensión:

$$A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\},$$

$$B = \{a, e, i\},$$

No es posible dar una definición por extensión de $\mathbb{R}$. $\diamondsuit$

Indicaremos con $\emptyset$ al **conjunto vacío**, es decir, al conjunto que no tiene elementos. El conjunto vacío puede ser definido por comprensión de diversas maneras, por ejemplo:

$$\emptyset = \{x : x \text{ es un número natural menor que } 0\}$$

$$\emptyset = \{x : x \text{ es una vocal que aparece en las palabras “día” y “noche”}\}$$

En cambio, su definición por extensión es $\emptyset = \{\}$.

Se dice que un conjunto A está **contenido** en un conjunto B, o que A es un **subconjunto** de B, y se escribe $A \subset B$, cuando todo elemento de A es elemento de B. Es decir,

$$A \subset B \leftrightarrow (\forall x)(x \in A \rightarrow x \in B)$$

Los conjuntos A y B son **iguales** cuando tienen exactamente los mismos elementos:

$$A = B \leftrightarrow (\forall x)(x \in A \leftrightarrow x \in B).$$

Proposición 25. *Sean A, B y C conjuntos cualesquiera. Se satisface que:*

1. $\emptyset \subset A \subset \mathbf{U}$
2. $A \subset A$ — *Propiedad reflexiva de la inclusión*
3. $(A \subset B \wedge B \subset A) \rightarrow A = B$ — *Propiedad antisimétrica de la inclusión*
4. $(A \subset B \wedge B \subset C) \rightarrow A \subset C$ — *Propiedad transitiva de la inclusión*
5. $A = A$ — *Propiedad reflexiva de la igualdad*
6. $A = B \rightarrow B = A$ — *Propiedad simétrica de la igualdad*
7. $(A = B \wedge B = C) \rightarrow A = C$ — *Propiedad transitiva de la igualdad*

Demostración: Probaremos los puntos 1. y 4., los demás quedan como ejercicios. Sea a un elemento cualquiera del universal. Por definición de $\emptyset$ sabemos que $a \in \emptyset$ es una proposición falsa, de donde

$$a \in \emptyset \rightarrow a \in A$$

es verdadera. Como a es un elemento cualquiera hemos probado que

$$(\forall x)(x \in \emptyset \rightarrow x \in A);$$

resulta, por la definición de contención, que $\emptyset \subset A$.
Para probar 4., asumamos que $A \subset B$ y que $B \subset C$. Sea a un elemento cualquiera de A,

$$\begin{aligned} a \in A \quad &\rightarrow a \in A \wedge A \subset B && \text{por adjunción} \\ &\rightarrow a \in B && \text{por definición de contención} \\ &\rightarrow a \in B \wedge B \subset C && \text{por adjunción} \\ &\rightarrow a \in C && \text{por definición de contención.} \end{aligned}$$

Como a es un elemento cualquiera de A, resulta $A \subset C$.
Hemos probado que

$$(A \subset B \wedge B \subset C) \rightarrow A \subset C.$$

□

Diremos que A es un **subconjunto propio** de B, y escribiremos $A \subsetneqq B$ cuando A está contenido en B y $A \neq B$, es decir,

$$A \subsetneqq B \leftrightarrow (A \subset B \wedge (\exists x)(x \in B \wedge x \notin A)).$$

Llamaremos **complemento** de A al conjunto que se denota A^c cuyos elementos son aquellos del universal que no pertenecen a A, es decir,

$$A^c = \{x :\sim x \in A\} = \{x : x \notin A\}.$$

Observar que para determinar explícitamente el complemento de un conjunto es necesario conocer el conjunto universal.

Ejemplo 26.

Si $A = \{x : x \in \mathbb{N} \wedge 1 \leq x\}$ y el conjunto universal es el conjunto de los números naturales $\mathbb{N}$, entonces $A^c = \emptyset$ pues todo elemento del universal está en A. En cambio, si el conjunto universal es el conjunto de los números enteros $\mathbb{Z}$ entonces $A^c = \{x : x \in \mathbb{Z} \wedge x \leq 0\} = \{0, -1, -2, -3, \cdots\} \neq \emptyset$. $\diamondsuit$

Proposición 27. *Sean A y B conjuntos cualesquiera. Se satisface que:*

1. $(A^c)^c = A \quad \emptyset^c = \mathbf{U} \quad \mathbf{U}^c = \emptyset$
2. $A \subset B \leftrightarrow B^c \subset A^c$

Demostración: Sea a un elemento cualquiera del universal,

$$\begin{aligned} a \in (A^c)^c &\leftrightarrow \sim a \in A^c && \text{por definición de complemento} \\ &\leftrightarrow \sim\sim a \in A && \text{por definición de complemento} \\ &\leftrightarrow a \in A && \text{por doble negación.} \end{aligned}$$

Hemos probado que $(A^c)^c = A$.

Por Proposición 25 (1.), todo conjunto está contenido en el universa, luego

$$\emptyset^c \subset \mathbf{U}. \tag{1.1}$$

Por otra parte, como

$$\begin{aligned} a \in \mathbf{U} &\rightarrow \sim a \in \emptyset && \text{por definición de vacío} \\ &\rightarrow a \in \emptyset^c && \text{por definición de complemento;} \end{aligned}$$

resulta que

$$\mathbf{U} \subset \emptyset^c. \tag{1.2}$$

De las relaciones (1.1) y (1.2), y la propiedad antisimétrica de la inclusión, obtenemos que $\emptyset^c = \mathbf{U}$.

Finalmente, como $\emptyset^c = \mathbf{U}$, obtenemos $(\emptyset^c)^c = \mathbf{U}^c$; y como $(\emptyset^c)^c = \emptyset$, resulta $\emptyset = \mathbf{U}^c$.

Ahora demostraremos el segundo punto del enunciado,

$$\begin{aligned}
A \subset B &\leftrightarrow (\forall x)(x \in A \to x \in B) && \text{por definición de inclusión}\\
&\leftrightarrow (\forall x)(\sim x \in B \to \sim x \in A) && \text{por equivalencia con contrarecíproco}\\
&\leftrightarrow (\forall x)(x \notin B \to x \notin A) && \text{por definición de } \notin\\
&\leftrightarrow (\forall x)(x \in B^c \to x \in A^c) && \text{por definición de complemento}\\
&\leftrightarrow B^c \subset A^c && \text{por definición de inclusión.}
\end{aligned}$$

□

Dado un conjunto A, $\mathcal{P}(A)$ denota al **conjunto de partes** de A. Los elementos de $\mathcal{P}(A)$ son los subconjuntos de A:

$$\mathcal{P}(A) = \{x : x \text{ es un subconjunto de } A\}.$$

Observar que los elementos del conjunto de partes son conjuntos. Si A tiene una cantidad n de elementos entonces $\mathcal{P}(A)$ tiene 2^n elementos.

Ejemplo 28.

- Si $A = \{1, 2, 3\}$ entonces

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

- Si $A = \{1\}$ entonces $\mathcal{P}(A) = \{\emptyset, \{1\}\}$.

  Como $\mathcal{P}(A)$ es un conjunto, podemos determinar su conjunto de partes:

$$\mathcal{P}(\mathcal{P}(A)) = \{\emptyset, \{\emptyset\}, \{\{1\}\}, \{\emptyset, \{1\}\}\}.$$

♢

Proposición 29. *Sean A y B conjuntos cualesquiera. Se satisface que:*

1. $A \in \mathcal{P}(A) \quad \emptyset \in \mathcal{P}(A) \quad \mathcal{P}(\emptyset) \neq \emptyset$
2. $A \subset B \leftrightarrow \mathcal{P}(A) \subset \mathcal{P}(B)$

Demostración: Por Proposición 25 (1.) y (2.), tenemos que $\emptyset \subset A$ y $A \subset A$; en consecuencia $\emptyset \in \mathcal{P}(A)$ y $A \in \mathcal{P}(A)$ por definición de conjunto de partes.

Como $\emptyset \subset \emptyset$, obtenemos $\emptyset \in \mathcal{P}(\emptyset)$; resulta que $\mathcal{P}(\emptyset) \neq \emptyset$.

Asumamos que $A \subset B$. Sea C un elemento cualquiera de $\mathcal{P}(A)$,

$$\begin{aligned}
C \in \mathcal{P}(A) &\rightarrow C \subset A, && \text{por definición de conjunto de partes}\\
&\rightarrow C \subset A \wedge A \subset B, && \text{por adjunción}\\
&\rightarrow C \subset B && \text{por transitividad de inclusión}\\
&\rightarrow C \in \mathcal{P}(B) && \text{por definición de conjunto de partes.}
\end{aligned}$$

Como C es un elemento cualquiera de $\mathcal{P}(A)$, resulta que $\mathcal{P}(A) \subset \mathcal{P}(B)$.

Hemos probado que

$$A \subset B \rightarrow \mathcal{P}(A) \subset \mathcal{P}(B). \qquad (1.3)$$

Ahora asumamos $\mathcal{P}(A) \subset \mathcal{P}(B)$. Sea a un elemento cualquiera de A.

$$\begin{aligned}
a \in A &\rightarrow \{a\} \subset A, && \text{por definición de inclusión}\\
&\rightarrow \{a\} \in \mathcal{P}(A), && \text{por definición de conjunto de partes}\\
&\rightarrow \{a\} \in \mathcal{P}(B) && \text{pues por hipótesis } \mathcal{P}(A) \subset \mathcal{P}(B)\\
&\rightarrow \{a\} \subset B && \text{por definición de conjunto de partes}\\
&\rightarrow a \in B && \text{por definición de inclusión.}
\end{aligned}$$

Como a es un elemento cualquiera de A, resulta que $A \subset B$.

Hemos probado que

$$\mathcal{P}(A) \subset \mathcal{P}(B) \rightarrow A \subset B. \qquad (1.4)$$

De las relaciones (1.3) y (1.4), obtenemos

$$A \subset B \leftrightarrow \mathcal{P}(A) \subset \mathcal{P}(B).$$

□

Ejercicio 30.

1. Probar que si $A \subset B$ y $B \subset C$ y $C \subset A$, entonces $A = B = C$.
2. Decir si son verdaderas o falsas las siguientes relaciones. Justifique.

   (a) $\emptyset \in \{\emptyset\}$ (b) $\emptyset \subset \{\emptyset\}$ (c) $\{\text{a}\} \in \{\text{a, b}\}$

   (d) $\emptyset \in \emptyset$ (e) $\{\text{a}\} \subset \{\text{a, b}\}$ (f) $\{\text{a, b}\} \in \{\text{a}, \{\text{a,b}\}\}$

   (g) $\{\emptyset\} \in \{\emptyset\}$ (h) $\{\text{a}\} \in \{\{\text{a}\}\}$ (i) $\{a, b\} \subset \{a, \{a, b\}\}$

3. Sea $A = \{2, \{x\}, \{\emptyset\}, \{2, x\}\}$, hallar $\mathcal{P}(A)$.
4. Hallar: $\mathcal{P}(\emptyset)$ y $\mathcal{P}(\mathcal{P}(\emptyset))$. $\diamondsuit$

Convención: con el objetivo de simplificar la notación, escribiremos

$$\{x \in A : p(x)\} \quad \text{en lugar de} \quad \{x : x \in A \wedge p(x)\}$$

para indicar el subconjunto de A formado por los elementos que satisfacen la propiedad p.

1.2.2. Operaciones entre conjuntos

Definiremos cuatro operaciones entre conjuntos: intersección, unión, diferencia y diferencia simétrica; y estudiaremos propiedades de cada una de ellas.
Dados conjuntos A y B, $A \cap B$ denota el **conjunto intersección** de A y B. Los elementos de $A \cap B$ son los elementos del universal que pertenecen a A y a B:

$$A \cap B = \{x : x \in A \wedge x \in B\}.$$

Ejemplo 31.

- Si $A = \{x \in \mathbb{N} : x \leq 20\}$ y $B = \{x \in \mathbb{N} : x \text{ es múltiplo de } 3\}$, entonces $A \cap B = \{3, 6, 9, 12, 15, 18\}$.
- Si $A = \{1, \{1\}\}$ entonces $\mathcal{P}(A) = \{\emptyset, \{1\}, \{\{1\}\}, \{1, \{1\}\}\}$. Resulta que $A \cap \mathcal{P}(A) = \{\{1\}\}$. ¿Porqué $1 \notin A \cap \mathcal{P}(A)$? ¿Porqué $\emptyset \notin A \cap \mathcal{P}(A)$? $\diamondsuit$

Los conjuntos A y B se dicen **disjuntos** cuando $A \cap B = \emptyset$.

Proposición 32. *Sean A, B y C conjuntos cualesquiera. Se satisface que:*

1. $A \cap A = A \quad A \cap \emptyset = \emptyset \quad A \cap \mathbf{U} = A$
2. $A \cap B \subset A$
3. $A \cap B = A \leftrightarrow A \subset B$
4. $A \cap B = B \cap A$ *Propiedad conmutativa de la intersección*
5. $(A \cap B) \cap C = A \cap (B \cap C)$ *Propiedad asociativa de la intersección*

Demostración: Probaremos los puntos 2., 3. y 5., los demás quedan como ejercicios. Sea a un elemento cualquiera de $A \cap B$.

$$\begin{aligned} a \in A \cap B &\rightarrow a \in A \wedge a \in B, && \text{por definición de } \cap \\ &\rightarrow a \in A && \text{por simplificación.} \end{aligned}$$

Como a es un elemento cualquiera de $A \cap B$, resulta que $A \cap B \subset A$.

Asumamos que $A \cap B = A$. Sea a un elemento cualquiera de A.

$$\begin{aligned} a \in A &\rightarrow a \in A \cap B && \text{pues por hipótesis } A \cap B = A \\ &\rightarrow (a \in A \wedge a \in B) && \text{por definición de intersección} \\ &\rightarrow a \in B && \text{por simplificación.} \end{aligned}$$

Como a es un elemento cualquiera de A, resulta que $A \subset B$.

Hemos probado que

$$A \cap B = A \rightarrow A \subset B. \tag{1.5}$$

Ahora, asumamos que $A \subset B$. Sabemos, por lo probado anteriormente, que $A \cap B \subset A$; luego, para probar que $A = A \cap B$, basta ver que $A \subset A \cap B$.

Sea a un elemento cualquiera de A.

$$\begin{aligned} a \in A &\rightarrow a \in B && \text{pues por hipótesis } A \subset B \\ &\rightarrow (a \in A \wedge a \in B) && \text{por adjunción} \\ &\rightarrow a \in A \cap B && \text{por definición de intersección} \end{aligned}$$

Como a es un elemento cualquiera de A, resulta que $A \subset A \cap B$; luego, hemos probado que

$$A \subset B \rightarrow A \cap B = A. \tag{1.6}$$

Con las implicaciones (1.5) y (1.6) queda demostrado el punto 3.

Sea a un elemento cualquiera del universal,

$$\begin{aligned} a \in (A \cap B) \cap C &\leftrightarrow (a \in A \cap B \wedge a \in C) && \text{por definición de intersección} \\ &\leftrightarrow ((a \in A \wedge a \in B) \wedge a \in C) && \text{por definición de intersección} \\ &\leftrightarrow (a \in A \wedge (a \in B \wedge a \in C)) && \text{por la asociatividad de } \wedge \\ &\leftrightarrow (a \in A \wedge a \in B \cap C) && \text{por definición de intersección} \\ &\leftrightarrow a \in A \cap (B \cap C) && \text{por definición de intersección} \end{aligned}$$

Como a es un elemento cualquiera del universal, resulta $(A \cap B) \cap C = A \cap (B \cap C)$.

□

Dados conjuntos A y B, $A \cup B$ denota el **conjunto unión** de A y B. Los elementos de $A \cup B$ son los elementos del universal que pertenecen a A o a B:

$$A \cup B = \{x : x \in A \vee x \in B\}.$$

Ejemplo 33.

- Si

$$A = \{x : x \text{ es una letra de la palabra “dado” } \} \text{ y}$$

$$B = \{x : x \text{ es una letra de la palabra “dedos”}\},$$

entonces $A \cup B = \{\text{d,a,o,e,s}\}$, mientras que $A \cap B = \{\text{d,o}\}$.

- Si $A = \{1\}$ y $B = \{2\}$ entonces $A \cup B = \{1, 2\}$ y $A \cap B = \emptyset$. Resulta que $\mathcal{P}(A) = \{\emptyset, \{1\}\}$; $\mathcal{P}(B) = \{\emptyset, \{2\}\}$; $\mathcal{P}(A \cup B) = \{\emptyset, \{1, \}, \{2\}, \{1, 2\}\}$; $\mathcal{P}(A \cap B) = \{\emptyset\}$; $\mathcal{P}(A) \cup \mathcal{P}(B) = \{\emptyset, \{1\}, \{2\}\}$; y $\mathcal{P}(A) \cap \mathcal{P}(B) = \{\emptyset\}$. Observar que $\mathcal{P}(A) \cup \mathcal{P}(B) \neq \mathcal{P}(A \cup B)$. ♢

Proposición 34. *Sean A, B y C conjuntos cualesquiera. Se satisface que:*

1. $A \cup A = A \quad A \cup \emptyset = A \quad A \cup \mathbf{U} = \mathbf{U}$
2. $A \subset A \cup B$
3. $A \cup B = A \leftrightarrow B \subset A$
4. $A \cup B = B \cup A$ *Propiedad conmutativa de la unión*
5. $(A \cup B) \cup C = A \cup (B \cup C)$ *Propiedad asociativa de la unión*
6. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *Propiedad distributiva de la intersección respecto de la unión*
7. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *Propiedad distributiva de la unión respecto de la intersección*

Demostración: Se deja como ejercicio. □

Dados conjuntos A y B, $A - B$ denota el **conjunto diferencia** entre A y B, también se llama A **menos** B. Los elementos de $A - B$ son los elementos de A que no pertenecen a B:

$$A - B = \{x : x \in A \wedge x \notin B\}.$$

Ejemplo 35.

Si $A = \{1, 2, 3, 6, 7, 8\}$, $B = \{2, 3, 4, 7, 8, 9\}$ y $C = \{3, 6, 9\}$, entonces

$$A - B = \{1, 6\} \quad B - A = \{4, 9\} \quad B - C = \{2, 4, 7, 8\}$$

$$(A - B) - C = \{1\} \quad A - (B - C) = \{1, 3, 6\}$$

Este ejemplo muestra que la diferencia entre conjuntos no satisface la propiedad conmutativa ni la propiedad asociativa. ♢

Proposición 36. *Sean A, B y C conjuntos cualesquiera. Se satisface que:*

1. $A - A = \emptyset \quad A - \emptyset = A \quad A - \mathbf{U} = \emptyset \quad \emptyset - A = \emptyset \quad \mathbf{U} - A = A^c$
2. $A - B \subset A$
3. $A - B = A \leftrightarrow A \cap B = \emptyset$
4. $(A - B) - C = (A - C) - B$
5. $A \cap (B - C) = (A \cap B) - (A \cap C)$ *Propiedad distributiva de la intersección respecto de la diferencia*

Demostración: Probaremos el punto 4., los demás quedan como ejercicios.

Sea a un elemento cualquiera del universal,

$$\begin{aligned}
a \in (A - C) - B &\leftrightarrow (a \in A - C \wedge a \notin B) && \text{por definición de diferencia}\\
&\leftrightarrow ((a \in A \wedge a \notin C) \wedge a \notin B) && \text{por definición diferencia}\\
&\leftrightarrow (a \in A \wedge (a \notin C \wedge a \notin B)) && \text{por asociatividad de la conjunción}\\
&\leftrightarrow (a \in A \wedge (a \notin B \wedge a \notin C)) && \text{por conmutatividad de la conjunción}\\
&\leftrightarrow ((a \in A \wedge a \notin B) \wedge a \notin C) && \text{por asociatividad de la conjunción}\\
&\leftrightarrow (a \in A - B \wedge a \notin C) && \text{por definición de diferencia}\\
&\leftrightarrow a \in (A - B) - C && \text{por definición de diferencia.}
\end{aligned}$$

□

Dados conjuntos A y B, $A \triangle B$ denota el **conjunto diferencia simétrica** entre A y B. Los elementos de $A \triangle B$ son los elementos del universal que pertenecen a uno de los conjuntos pero no al otro:

$$A\triangle B = \{x : (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}.$$

Ejemplo 37.

Si $A = \{1, 3, 5, 7, 9\}$ y $B = \{2, 3, 6, 7, 10\}$ entonces $A\triangle B = \{1, 2, 5, 6, 9, 10\}$. ♢

Proposición 38. *Sean A, B y C conjuntos cualesquiera. Se satisface que:*

1. $A\triangle A = \emptyset \quad A\triangle\emptyset = A \quad A\triangle \mathbf{U} = A^c$
2. $A\triangle B = (A \cup B) - (A \cap B)$
3. $A\triangle B \subset A \cup B$
4. $A\triangle B = A \leftrightarrow B = \emptyset$
5. $A\triangle B = B\triangle A$ *Propiedad conmutativa de la diferencia simétrica*
6. $(A\triangle B)\triangle C = A\triangle(B\triangle C)$ *Propiedad asociativa de la diferencia simétrica*
7. $A \cap (B\triangle C) = (A \cap B)\triangle(A \cap C)$ *Propiedad distributiva de la intersección respecto de la diferencia simétrica*

Demostración: Probaremos el punto 4., los restantes quedan como ejercicios.
Asumamos que $A\triangle B = A$. Probaremos que $B = \emptyset$ por el absurdo: supongamos existe $b \in B$;

$$\begin{aligned}
b \in B &\rightarrow (b \in B \wedge (b \in A \vee b \notin A)) && \text{por adjunción;}\\
&\rightarrow ((b \in B \wedge b \in A) \vee (b \in B \wedge b \notin A)) && \text{por propiedad distributiva;}\\
&\rightarrow ((b \notin A\triangle B \wedge b \in A) \vee (b \in A\triangle B \wedge b \notin A)) && \text{por definición de diferencia simétrica;}\\
&\rightarrow ((b \notin A \wedge b \in A) \vee (b \in A \wedge b \notin A)) && \text{por hipótesis } A\triangle B = A\\
&\rightarrow (b \notin A \wedge b \in A).
\end{aligned}$$

La conclusión $(b \notin A \wedge b \in A)$ es una contradicción que proviene de suponer la existencia de b; resulta que un tal b no puede existir, es decir, $B = \emptyset$.
Hemos probado que

$$A\triangle B = A \rightarrow B = \emptyset. \tag{1.7}$$

Ahora asumamos que $B = \emptyset$;

$$\begin{aligned}
B = \emptyset &\rightarrow A\triangle B = A\triangle\emptyset && \text{por igualdad}\\
&\rightarrow A\triangle B = A && \text{pues } A\triangle\emptyset = A.
\end{aligned}$$

Hemos probado que

$$B = \emptyset \to A \triangle B = A. \qquad (1.8)$$

De las relaciones (1.7) y (1.8) resulta

$$A \triangle B = A \leftrightarrow B = \emptyset.$$

□

Ejercicio 39.

Sean A y B conjuntos cualesquiera, probar que se satisfacen las siguientes relaciones.

1. $(A \cup B)^c = A^c \cap B^c$ $\qquad (A \cap B)^c = A^c \cup B^c$ $\qquad$ Leyes de De Morgan
2. $\mathcal{P}(A) \cup \mathcal{P}(B) \subset \mathcal{P}(A \cup B)$
3. $A \cap B = \emptyset \leftrightarrow \mathcal{P}(A) \cap \mathcal{P}(B) = \{\emptyset\}$
4. $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B) \leftrightarrow (A \subset B \vee B \subset A)$
5. $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$
6. $(A \triangle B) \cup (A \cap B) = A \cup B$ ♢

1.2.3. Familias de Conjuntos

Cuando necesitamos nombrar varios conjutos podemos utilizar **subíndices**.

Ejemplo 40.

- Para cada natural n, sea $A_n = \{x \in \mathbb{R} : x > n\}$.

  De esta forma estamos nombrando una cantidad infinita de conjuntos:

  $A_1 = \{x \in \mathbb{R} : x > 1\}$;

  $A_2 = \{x \in \mathbb{R} : x > 2\}$;

  $A_3 = \{x \in \mathbb{R} : x > 3\}$;

  $\vdots$

  Con $(A_n)_{n \in \mathbb{N}}$ indicamos a la familia formada por todos estos conjuntos.

- Sea $A = \{1, a, 2, b, 3, c\}$. Para cada elemento x de A sea $B_x = A - \{x\}$. De esta forma estamos nombrando los siguientes conjuntos:

  $B_1 = A - \{1\} = \{a, 2, b, 3, c\}$;

  $B_a = A - \{a\} = \{1, 2, b, 3, c\}$;

  $B_2 = A - \{2\} = \{1, a, b, 3, c\}$;

  $B_b = A - \{b\} = \{1, a, 2, 3, c\}$;

$B_3 = A - \{3\} = \{1, a, 2, b, c\}$; y

$B_c = A - \{c\} = \{1, a, 2, b, 3\}$.

Con $(B_x)_{x \in A}$ indicamos a la familia cuyos miembros son los seis conjuntos listados anteriormente. ♢

En general, dado un conjunto no vacío I, que llamaremos **conjunto de subíndices**, $(A_i)_{i \in I}$ denota la **familia de conjuntos** cuyos **miembros** son cada uno de los conjuntos A_i con $i \in I$.

Mediante $\bigcup_{i \in I} A_i$ indicaremos al **conjunto unión de los miembros de la familia** definido de la siguiente manera:

$$\bigcup_{i \in I} A_i = \{x : \text{ existe } i \in I \text{ tal que } x \in A_i\}.$$

Análogamente, $\bigcap_{i \in I} A_i$ denota el **conjunto intersección de los miembros de la familia**,

$$\bigcap_{i \in I} A_i = \{x : x \in A_i \text{ para todo } i \in I\}.$$

Ejemplo 41.

Para las familias $(A_n)_{n \in \mathbb{N}}$ y $(B_x)_{x \in A}$ del ejemplo anterior, vale que

$$\bigcup_{n \in \mathbb{N}} A_n = A_1 \qquad \bigcap_{n \in \mathbb{N}} A_n = \emptyset.$$

$$\bigcup_{x \in A} B_x = A \qquad \bigcap_{x \in A} B_x = \emptyset.$$

♢

Una **partición** de un conjunto A es una familia de conjuntos $(A_i)_{i \in I}$ con subíndices en un conjunto I cualquiera, que satisface cada una de las siguientes condiciones:

1. $A_i \neq \emptyset$ para todo $i \in I$;
2. $A_i \cap A_j = \emptyset$ para todo par de subíndices i y j, $i \neq j$, de I;
3. $\bigcup_{i \in I} A_i = A$.

Ejemplo 42.

Las siguientes son dos particiones distintas del conjunto de los números reales:

- La familia de conjuntos $(A_m)_{m\in\mathbb{Z}}$ con $A_m = \{x \in \mathbb{R} : m < x \leq m+1\}$.
- La familia de conjuntos con los siguientes tres miembros: $A_1 = \{x \in \mathbb{R} : x < 0\}$, $A_2 = \{0\}$ y $A_3 = \{x \in \mathbb{R} : x > 0\}$. ♢

Ejercicio 43.

1. Determinar la unión y la intersección de las siguientes familias de conjuntos
   a) $A_n = \{-n, 0, n\}$ $\quad n \in \mathbb{Z}$
   b) $B_n = \{x \in \mathbb{N} : x \text{ es múltiplo de } n\}$ $\quad n \in \mathbb{N}$
2. Sea A un conjunto y $(A_i)_{i\in I}$ una familia de conjuntos. Probar que

$$A \cup \bigcup_{i\in I} A_i = \bigcup_{i\in I}(A \cup A_i)$$

$$A \cap \bigcup_{i\in I} A_i = \bigcup_{i\in I}(A \cap A_i).$$

3. Indicar todas la particiones que se pueden dar el conjunto $A = \{1, 2, 3\}$. ♢

Capítulo 2

Relaciones y Funciones

2.0.4. Producto cartesiano y relaciones

Dados dos elementos cualesquiera a y b, mediante (a, b) indicaremos el **par ordenado** con **primera coordenada** a y **segunda coordenada** b. Diremos que dos pares ordenados son iguales cuando sus primeras coordenadas son iguales y sus segundas coordenadas también lo son, es decir:

$$(a, b) = (a', b') \leftrightarrow (a = a' \ \wedge \ b = b').$$

Sean A y B conjuntos. Representaremos con $A \times B$ el **producto cartesiano** de A por B definido como el conjunto de los pares ordenados con primera coordenada perteneciente a A y segunda coordenada perteneciente a B:

$$A \times B = \{(x, y) : x \in A \wedge y \in B\}.$$

Ejemplo 44.

- $(3 + 2, -1) = (5, -1) \qquad (3, 2) \neq (2, 3) \qquad (-1, 1) \neq (1, -1).$
- Si $A = \{1, 2, 3\}$ y $B = \{1, 5\}$ entonces

$$A \times B = \{(1, 1), (1, 5), (2, 1), (2, 5), (3, 1), (3, 5)\}$$

$$(1, 3) \notin A \times B \qquad (1, 3) \in B \times A$$

$$(A \times B) \cap (B \times A) = \{(1, 1)\}.$$



Proposición 45. *Sean A, B y C conjuntos cualesquiera. Se satisface que,*

1. $A \times \emptyset = \emptyset \times A = \emptyset$.
2. *Si A y B son no vacíos,* $A \times B = B \times A \leftrightarrow A = B$.
3. *Si A y B son no vacíos,* $A \times B \subset C \times D \leftrightarrow A \subset C \wedge B \subset D$.
4. $(A \times B) \cup (C \times D) \subset (A \cup C) \times (B \cup D)$.
5. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

Demostración: Probaremos el punto 2), los restantes quedan como ejercicios.

Asumamos que $A \times B = B \times A$. Sea a un elemento cualquiera de A. Como $B \neq \emptyset$, existe un elemento $b \in B$.

$a \in A$	$\rightarrow$	$(a, b) \in A \times B$	por definición de producto cartesiano
	$\rightarrow$	$(a, b) \in B \times A$	pues por hipótesis $A \times B = B \times A$
	$\rightarrow$	$a \in B \wedge b \in A$	por definición de producto cartesiano
	$\rightarrow$	$a \in B$	por simplificación.

Hemos probado que

$$A \subset B. \tag{2.1}$$

Análogamente, sea b un elemento cualquiera de B. Como $A \neq \emptyset$, existe un elemento $a \in A$.

$b \in B$	$\rightarrow$	$(a, b) \in A \times B$	por definición de producto cartesiano
	$\rightarrow$	$(a, b) \in B \times A$	pues por hipótesis $A \times B = B \times A$
	$\rightarrow$	$a \in B \wedge b \in A$	por definición de producto cartesiano
	$\rightarrow$	$b \in A$	por simplificación.

Hemos probado que

$$B \subset A. \tag{2.2}$$

De (2.1) y (2.2) resulta $A = B$; en consecuencia hemos probado que para A y B no vacíos se satisface que

$$A \times B = B \times A \rightarrow A = B.$$

La implicación recíproca es trivial. □

Sean A y B conjuntos. Una **relación de** A **en** B es un subconjunto del producto cartesiano de A por B; es decir:

$$\mathcal{R} \text{ es una relación de A en B } \leftrightarrow \mathcal{R} \subset A \times B.$$

Si $(a,b) \in \mathcal{R}$ se dice que a está **$\mathcal{R}$-relacionado** con b o que a está relacionado con b por $\mathcal{R}$; y suele notarse $a\mathcal{R}b$. Si $(a,b) \notin \mathcal{R}$ se dice que a no está $\mathcal{R}$-relacionado con b y se escribe $a \not\mathcal{R} b$.

Tal como un conjunto cualquiera, una relación puede ser definida por extensión o por comprensión.

Ejemplo 46.

- Si $A = \{1,2,3\}$ y $B = \{a,b,c,d\}$, entonces $\mathcal{R} = \{(1,a),(2,c),(2,a)\}$ es una relación de A en B. Esta relación vincula a 1 con a; a 2 con c y con a; y no vincula a 3 con ningún elemento de B.

  Otra forma de representar la relación $\mathcal{R}$ es escribiendo los pares relacionados separados por el símbolo $\mathcal{R}$:

  $$1\mathcal{R}a \;\; 2\mathcal{R}c \;\; 2\mathcal{R}a$$

  Otra relación de A en B es $\mathcal{T} = \{(3,a),(3,b),(3,c),(3,d)\}$. Esta relación vincula a 3 con cada elemento de B, en tanto que 1 y 2 no están relacionados con elemento alguno de B.
- Sea A el conjunto de las ciudades de Argentina y B es el conjunto de las provincias de Argentina. Las siguientes son dos relaciones de A en B:

  $$\mathcal{C} = \{(x,y) \in A \times B : x \text{ es la capital de } y\};$$

  $$\mathcal{D} = \{(x,y) \in A \times B : x \text{ es una ciudad de la provincia } y\}.$$

  Es claro que, por ejemplo, el par (La Plata, Buenos Aires)$\in \mathcal{C} \cap \mathcal{D}$; en cambio (Lincoln, Buenos Aires)$\notin \mathcal{C}$ y (Lincoln, Buenos Aires)$\in \mathcal{D}$.

  Alternativamente, las relaciones anteriores pueden ser descriptas de la siguiente forma:

  Sean $\mathcal{C}$ y $\mathcal{D}$ las relaciones entre ciudades y provincias de Argentina dadas respectivamente por,

  $$x\,\mathcal{C}\,y \leftrightarrow x \text{ es la capital de } y;$$

$$x\,\mathcal{D}\,y \leftrightarrow x \text{ es una ciudad de la provincia } y.$$

- Algunas relaciones suelen no ser expresadas con la notación de conjuntos. Tal es el caso de la relación "menor o igual" de $\mathbb{R}$ en $\mathbb{R}$. Cuando escribimos $\sqrt{2} \leq 2$ estamos indicando que el par $(\sqrt{2}, 2)$ pertenece a la relación "menor o igual". Algo similar ocurre con la relación "contenido" de $\mathcal{P}(U)$ en $\mathcal{P}(U)$: cuando escribimos $A \subset B$ estamos indicando que el par (A, B) pertenece a la relación "contenido".
- Sea $A = \{1, 2, 3, 4, 5\}$. Llamemos $\sim$ a la relación de A en A dada por

$$x \sim y \leftrightarrow x + y = 8.$$

Esta relación es el conjunto

$$\{(x, y) \in A \times A : x + y = 8\} = \{(3, 5), (4, 4), (5, 3)\}.$$

$\diamondsuit$

Sea $\mathcal{R}$ una relación de A en B. El conjunto A se dice el **conjunto de partida** de $\mathcal{R}$; y el conjunto B se dice el **conjunto de llegada** o **codominio** de $\mathcal{R}$.
El conjunto

$$Dom(\mathcal{R}) = \{x \in A : \text{ existe } y \in B \text{ tal que } (x, y) \in \mathcal{R}\}$$

es el **dominio** de $\mathcal{R}$; y el conjunto

$$Img(\mathcal{R}) = \{y \in B : \text{ existe } x \in A \text{ tal que } (x, y) \in \mathcal{R}\}$$

es el **rango** o **imagen** de $\mathcal{R}$.
Se llama **relación inversa** de $\mathcal{R}$ a la relación de B en A dada por

$$\mathcal{R}^{-1} = \{(y, x) : (x, y) \in \mathcal{R}\}.$$

Dado $A' \subset A$, se llama **imagen de** A' por $\mathcal{R}$ al conjunto

$$\mathcal{R}(A') = \{y \in B : \text{ existe } x \in A' \text{ tal que } (x, y) \in \mathcal{R}\}.$$

Dado $B' \subset B$, se llama **imagen inversa de** B' por $\mathcal{R}$ a la imagen de B' por $\mathcal{R}^{-1}$; es decir: al conjunto

$$\mathcal{R}^{-1}(B') = \{x \in A : \text{ existe } y \in B' \text{ tal que } (x, y) \in \mathcal{R}\}.$$

Ejemplo 47.
Si $A = \{1, 2, 3\}$, $B = \{a, b, c, d\}$ y $\mathcal{R} = \{(1, a), (2, c), (2, a)\}$, entonces

$$Dom(\mathcal{R}) = \{1, 2\} \quad \text{y} \quad Img(\mathcal{R}) = \{a, c\}.$$

Observar que $3 \notin Dom(\mathcal{R})$ pues 3 no está relacionado con ningún elemento de B: $(3, a) \notin \mathcal{R}$, $(3, b) \notin \mathcal{R}$, $(3, c) \notin \mathcal{R}$ y $(3, d) \notin \mathcal{R}$. Por otro lado, $b \notin Img(\mathcal{R})$ pues no existe un elemento de A relacionado con b: $(1, b) \notin \mathcal{R}$, $(2, b) \notin \mathcal{R}$ y $(3, b) \notin \mathcal{R}$.
Si $A' = \{2, 3\}$, $A'' = \{3\}$, $B' = \{a, d\}$ y $B'' = \{b, d\}$, entonces

$$\mathcal{R}(A') = \{a, c\} \qquad \mathcal{R}(A'') = \emptyset$$

$$\mathcal{R}^{-1}(B') = \{1, 2\} \qquad \mathcal{R}^{-1}(B'') = \emptyset.$$

♢

Proposición 48. *Sea $\mathcal{R}$ una relación de A en B. Se satisface que,*

1. $(\mathcal{R}^{-1})^{-1} = \mathcal{R}$.
2. $Dom(\mathcal{R}^{-1}) = Img(\mathcal{R})$.
3. $Img(\mathcal{R}^{-1}) = Dom(\mathcal{R})$.

Demostración: Demostraremos el punto 2), los restantes quedan como ejercicios. Sea y un elemento cualquiera,

$$\begin{aligned} y \in Img(\mathcal{R}) &\leftrightarrow y \in B \wedge \text{ existe } x \in A \text{ tal que } (x, y) \in \mathcal{R} && \text{por def. de } Img \\ &\leftrightarrow y \in B \wedge \text{ existe } x \in A \text{ tal que } (y, x) \in \mathcal{R}^{-1} && \text{por def. de } \mathcal{R}^{-1} \\ &\leftrightarrow y \in Dom(\mathcal{R}^{-1})) && \text{por def. de} Dom. \end{aligned}$$



Sea $\sim$ una **relación en un conjunto** A, esto es, una relación de A en A: el conjunto de partida y el conjunto de llegada de $\sim$ son el mismo conjunto A.

La relación $\sim$ se dice **reflexiva** si para todo $x \in A$ se verifica que

$$x \sim x.$$

La relación $\sim$ se dice **simétrica** si para todo $x \in A$ y para todo $y \in A$ se verifica que

$$x \sim y \to y \sim x.$$

La relación $\sim$ se dice **antisimétrica** si para todo $x \in A$ y para todo $y \in A$ se verifica que

$$(x \sim y \wedge y \sim x) \to x = y.$$

La relación $\sim$ se dice **transitiva** si para todo $x \in A$, para todo $y \in A$ y para todo $z \in A$ se verifica que

$$(x \sim y \wedge y \sim z) \to x \sim z.$$

Ejemplo 49.

Sea $\sim$ la relación definida en $\mathbb{N}$ en la forma

$$n \sim m \leftrightarrow n < m$$

Esta relación no es reflexiva pues, por ejemplo, $1 \nsim 1$.

Tampoco es simétrica pues, por ejemplo, $1 \sim 2$ pero $2 \nsim 1$.

La relación es antisimétrica puesto que dados elementos cualesquiera n y m de $\mathbb{N}$,

$$(n < m \wedge m < n) \to n = m$$

es verdadera porque el antecedente es falso. $\diamondsuit$

Ejercicio 50.

Sea $\mathcal{R}$ una relación en un conjunto A. Probar que

1. $\mathcal{R} \cup \mathcal{R}^{-1}$ es simétrica.
2. Si $\mathcal{R}$ reflexiva $\to \mathcal{R}^{-1}$ es reflexiva.
3. Si $\mathcal{R}$ simétrica $\to \mathcal{R}^{-1}$ es simétrica.
4. Si $\mathcal{R}$ transitiva $\to \mathcal{R}^{-1}$ es transitiva.
5. Si $\mathcal{R}$ antisimétrica $\to \mathcal{R}^{-1}$ es antisimétrica.
6. Sea $B \subset A$. Se llama **restricción** de $\mathcal{R}$ a B a la relación $\mathcal{R}_B$ definida en B en la forma
$$\mathcal{R}_B = \{(x, y) \in \mathcal{R} : (x, y) \in B \times B\}.$$

Probar que si $\mathcal{R}$ es reflexiva, simétrica, antisimétrica o transitiva, entonces $\mathcal{R}_B$ lo es. ¿Vale la implicación recíproca? $\diamondsuit$

2.0.5. Relaciones de orden

Una relación $\sim$ en un conjunto A se dice **relación de orden** si es reflexiva, antisimétrica y transitiva. Si además, para todo $x \in A$ y para todo $y \in A$, se verifica que

$$x \sim y \vee y \sim x,$$

entonces la relación se dice de **orden total** .

Ejemplo 51.

- La relación $\leq$ en $\mathbb{R}$ es una relación de orden total. Nos referiremos a esta relación como "el orden usual de $\mathbb{R}$".
- Sea E es un conjunto cualquiera. La relación de inclusión $\subset$ es una relación de orden en $\mathcal{P}(E)$. Si E tiene al menos dos elementos, $\subset$ no es un orden total. Efectivamente, asumamos que a y b son elementos de E y $a \neq b$. Así, $\{a\} \in \mathcal{P}(E)$ y $\{b\} \in \mathcal{P}(E)$, pero

$$\{a\} \not\subset \{b\} \quad \wedge \{b\} \not\subset \{a\}.$$

- Sea $\mathcal{R}$ una relación de orden en A y $\mathcal{S}$ es una relación de orden en B. Se define en $A \times B$ la relación $\sim$ en la forma:

$$(a, b) \sim (a', b') \leftrightarrow (a\mathcal{R}a' \wedge b\mathcal{S}b')$$

La relación $\sim$ es una relación de orden en $A \times B$; se llama **orden producto** de $\mathcal{R}$ y $\mathcal{S}$. Efectivamente,

$\sim$ es reflexiva:

$$\begin{array}{lll} (a,b) \in A \times B & \rightarrow (a \in A \wedge b \in B) & \text{por definición de } A \times B \\ & \rightarrow (a\mathcal{R}a \wedge b\mathcal{S}b) & \text{pues } \mathcal{R} \text{ y } \mathcal{S} \text{ son reflexivas} \\ & \rightarrow (a,b) \sim (a,b) & \text{por definición de } \sim . \end{array}$$

$\sim$ es antisimétrica:

$$\begin{aligned}((a,b)\sim(a',b') \wedge (a',b')\sim(a,b)) &\rightarrow ((a\mathcal{R}a' \wedge b\mathcal{S}b') \wedge (a'\mathcal{R}a \wedge b'\mathcal{S}b))\\ &\quad\ \text{por definición de } \sim\\ &\rightarrow ((a\mathcal{R}a' \wedge a'\mathcal{R}a) \wedge (b\mathcal{S}b' \wedge b'\mathcal{S}b))\\ &\quad\ \text{por asociat. y conmutat. de } \wedge\\ &\rightarrow (a=a' \wedge b=b')\\ &\quad\ \text{pues } \mathcal{R} \text{ y } \mathcal{S} \text{ son antisimétricas}\\ &\rightarrow (a,b)=(a',b')\\ &\quad\ \text{por definición de par ordenado.}\end{aligned}$$

$\sim$ es transitiva:

$$\begin{aligned}((a,b)\sim(a',b') \wedge (a',b')\sim(a'',b'')) &\rightarrow ((a\mathcal{R}a' \wedge b\mathcal{S}b') \wedge (a'\mathcal{R}a'' \wedge b'\mathcal{S}b''))\\ &\quad\ \text{por definición de } \sim\\ &\rightarrow ((a\mathcal{R}a' \wedge a'\mathcal{R}a'') \wedge (b\mathcal{S}b' \wedge b'\mathcal{S}b''))\\ &\quad\ \text{por asociat. y conmutat. de } \wedge\\ &\rightarrow (a\mathcal{R}a'' \wedge b\mathcal{S}b'')\\ &\quad\ \text{pues } \mathcal{R} \text{ y } \mathcal{S} \text{ son transitivas}\\ &\rightarrow (a,b)\sim(a'',b'')\\ &\quad\ \text{por definición de } \sim .\end{aligned}$$

- Si $\mathcal{R}$ es una relación de orden en A y $B \subset A$, entonces la restricción de $\mathcal{R}$ a B también es una relación de orden en B; se dice el **orden inducido** por $\mathcal{R}$ en B. Por ejemplo: $\leq$ es una relación de orden en $\mathbb{R}$ y, en consecuencia, induce un orden en cualquier subconjunto de $\mathbb{R}$. $\diamondsuit$

Sean x e y elementos distintos entre sí de un conjunto ordenado por una relación $\sim$. Por analogía con lo que ocurre con la relación "menor o igual" en el conjunto $\mathbb{R}$, se dice que

- x es **menor** que y, o que y es **mayor** que x, cuando $x \sim y$;
- y es **consecutivo** de x cuando $x \sim y$ y, para todo $z \in A$,

$$x \sim z \sim y \rightarrow (x = z \vee y = z).$$

Un conjunto ordenado y con una cantidad finita de elementos puede representarse mediante un **diagrama de Hasse**: a cada elemento del conjunto se le hace corresponder un punto del plano de forma tal que si x es menor que y el punto correspondiente

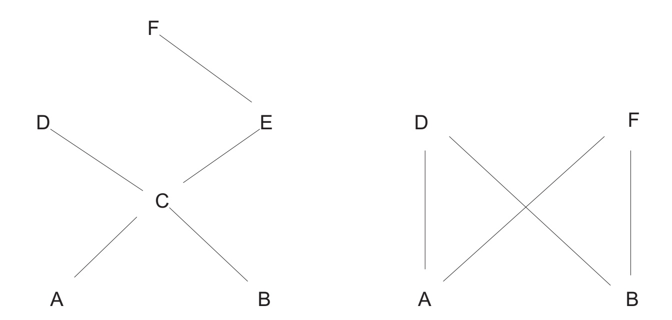


Figura 2.1: Diagramas de Hasse de las relaciones $\mathcal{R}$ y $\mathcal{R}_S$, respectivamente, del Ejemplo 52.

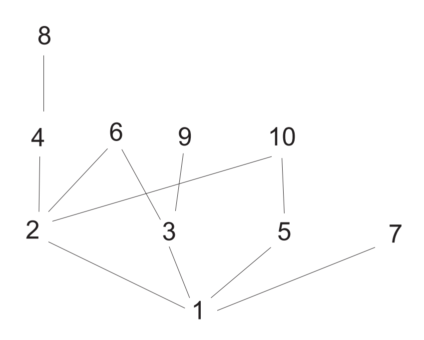


Figura 2.2: Diagrama de Hasse de la relación $\sim$ del Ejemplo 52.

a x está por debajo del punto correspondiente a y. Luego dos puntos se unen con una línea si uno es consecutivo del otro.

Ejemplo 52.

- El diagrama de Hasse representado a la izquierda en la Figura 2.1, correponde a la relación de orden $\mathcal{R}$ definida en el conjunto $\{A, B, C, D, E, F\}$ por los pares ordenados: (A, A); (A, C); (A, D); (A, E); (A, F); (B, B); (B, C); (B, D); (B, E); (B, F); (C, C); (C, D); (C, E); (C, F); (D, D); (E, E); (E, F); (F, F). El orden $\mathcal{R}_S$ inducido por $\mathcal{R}$ en el subconjunto $S = \{A, B, D, F\}$ es la relación definida por los pares ordenados (A, A); (A, D); (A, F); (B, B); (B, D); (B, F); (D, D); (F, F). El diagrama de Hasse de $\mathcal{R}_S$ se muestra en la Figura 2.1.
- El diagrama de Hasse correspondiente a la relación $\sim$ definida en el conjunto $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ en la forma

$$x \sim y \leftrightarrow x \text{ divide a } y,$$

es el representado a la derecha en la Figura 2.2.



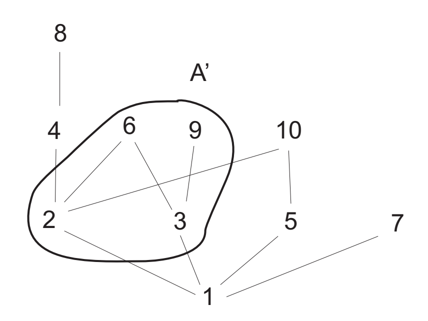


Figura 2.3: Subconjunto A' del Ejemplo 53.

Sea A' un subconjunto no vacío de un conjunto A ordenado por una relación $\sim$ y sea $a \in A$.

- a es **maximal** en A' si $a \in A'$ y en A' no hay un elemento mayor que a; es decir: $a \in A'$ y para todo $x \in A'$ se verifica que si $a \sim x$ entonces $x = a$.
- a es **minimal** en A' si $a \in A'$ y en A' no hay un elemento menor que a; es decir: $a \in A'$ y para todo $x \in A'$ se verifica que si $x \sim a$ entonces $x = a$.
- a es una **cota superior** de A' si a es mayor o igual que todos los elementos de A'; es decir: para todo $x \in A'$ se verifica que $x \sim a$.
- a es una **cota inferior** de A' si a es menor o igual que todos los elementos de A'; es decir: para todo $x \in A'$ se verifica que $a \sim x$.
- a es **primer elemento** de A' si $a \in A'$ y a es cota inferior de A'.
- a es **último elemento** de A' si $a \in A'$ y a es cota superior de A'.
- a es **supremo** de A' si a es el primer elemento del conjunto de las cotas superiores de A; es decir: a es el primer elemento del conjunto

$$\{x \in A : \text{ es cota superior de } A'\}.$$

- a es **ínfimo** de A', si a es el último elemento del conjunto de las cotas inferiores de A; es decir: a es el último elemento del conjunto

$$\{x \in A : x \text{ es cota inferior de } A'\}.$$

Ejemplo 53.

- Consideremos el subconjunto $A' = \{2, 3, 6, 9\}$ del conjunto ordenado representado en la Figura 2.3 mediante su diagrama de Hasse.

2 no es maximal en A', pues en A' hay elementos mayores que 2, por ejemplo 6.

6 y 9 son maximales en A'.

4 no es maximal en A', pues $4 \notin A'$.

No hay cotas superiores de A':

8 no es cota superior, pues, por ejemplo, 8 no es mayor que 6;

6 no es cota superior, pues, por ejemplo, 6 no es mayor que 9;

y así con los restantes elementos.

Como A' no admite cotas superiores entonces tampoco tiene último elemento ni supremo.

2 es minimal en A', pues $2 \in A'$ y en A' no hay elementos menores que 2. Pero 2 no es cota inferior de A', pues 2 no es menor que el elemento 3 de A'.

Analogamente, 3 es un elemento minimal de A', pero no es cota inferior de A'.

1 no es minimal en A', pues $1 \notin A'$.

1 es cota inferior de A', pues 1 es menor que 2, que 3, que 6 y que 9.

1 es la única cota inferior de A', es decir, el conjunto de las cotas inferiores de A' es $\{1\}$.

A' no tiene primer elemento, pues la única cota inferior no pertenece a A'.

1 es ínfimo de A', pues es el último elemento del conjunto $\{1\}$.

- Consideremos en $\mathbb{R}$ el orden usual y sea A' el intervalo $(2, 5]$.

  5 es un elemento maximal de A', pues $5 \in A'$ y en A' no hay ningún elmento mayor que 5.

  5 es cota superior de A', pues 5 es mayor o igual que todo elemento de A'.

  A' admite muchas cotas superiores; el conjunto formado por todas las cotas superiores de A' es el intervalo $[5, \infty)$.

  5 es último elemento de A', pues $5 \in A'$ y 5 es cota superior de A'.

  5 es supremo de A', pues 5 es el primer elemento del conjunto $[5, \infty)$ formado por las cotas superiores de A'.

  2 no es un elemento minimal de A', pues $2 \notin A'$.

  2 es cota inferior de A', pues 2 es menor o igual que todo elemento de A'.

  A' admite muchas cotas inferiores; el conjunto formado por todas las cotas inferiores de A' es el intervalo $(-\infty, 2]$.

A' no tiene primer elemento, pues ninguna de las cotas inferiores pertence a A'. 2 es ínfimo de A', pues 2 es el último elemento del conjunto $(-\infty, 2]$ formado por las cotas inferiores de A'. $\diamondsuit$

Proposición 54. *Se cumple que:*

1. *Si a es primer (último) elemento de A' entonces a es minimal (maximal) de A'.*
2. *Si a es primer (último) elemento de A' entonces a es ínfimo (supremo) de A'.*
3. *Si a y a' son primeros (últimos) elementos de A' entonces $a = a'$. En otras palabras: el primer (último) elemento, si existe, es único.*
4. *Si a y a' son ínfimos (supremos) de A' entonces $a = a'$. En otras palabras: el ínfimo (supremo), si existe, es único.*

Demostración: 1. Asumamos que a es primer elemento de A'.
Por definición de primer elemento,

$$a \in A'. \tag{2.3}$$

Por otro lado, también por definición de primer elemento, a es cota inferior de A', luego a es menor o igual que cualquier elemento de A'; resulta que

$$\text{en } A' \text{ no hay elementos menores que } a. \tag{2.4}$$

De (2.3) y (2.4) se desprende que a es un elemento minimal de A'.
2. Asumamos que a es primer elemento de A'. Por definición de primer elemento

$$a \in C, \tag{2.5}$$

donde C es el conjunto de las cotas inferiores de A'. Veremos a continuación que a es el último elemento de C.
Sea x un elemento cualquiera de C. Como x es cota inferior de A' y $a \in A'$, entonces $x \sim a$, donde $\sim$ es la relación de orden. Hemos probado que, para todo x,

$$x \in C \to x \sim a. \tag{2.6}$$

De (2.5) y (2.6) resulta que $a \in C$ y a cota superior de C, respectivamente; entonces a es último elemento de C, es decir, a es ínfimo de A'.

La demostración de los restantes puntos queda como ejercicio. □

Una relación de orden $\sim$ en un conjunto A se dice un **buen orden** si todo subconjunto no vacío de A tiene primer elemento.

Ejemplo 55.

- El orden representado en el diagrama de Hasse de la Figura 2.2 no es un buen orden: el subconjunto $\{6, 7\}$ no tiene primero elemento.
- En $\mathbb{R}$, la relación $\leq$ no es un buen orden: cualquier intervalo no vacío abierto a izquierda no tiene primer elemento. ♢

Proposición 56. *Todo buen orden es orden total.*

Demostración: Asumamos que $\sim$ es un buen orden en un conjunto A. Sean a y b elementos cualquiera de A. Veremos que $a \sim b$ o $b \sim a$.

Sea $A' = \{a, b\}$. Como $\sim$ es un buen orden en A y A' es un subconjunto no vacío de A, A' tiene primer elemento. Resulta que a es primer elemento de A' o b primer elemento de A', pues en A' no hay otros elementos. Luego, por definición de primer elemento, $a \sim b$ o $b \sim a$. Como a y b son elemento cualesquiera de A, hemos probado que $\sim$ es un orden total. □

Ejercicio 57.

1. Considere en el conjunto $\mathbb{N} \times \mathbb{N}$ la relación $\diamondsuit$ definida por

$$(n, m)\diamondsuit(s, t) \Leftrightarrow n \leq s$$

   Analice las propiedades de esta relación. ¿Es de orden? ¿Puede dar otra relación con la que $\mathbb{N} \times \mathbb{N}$ resulte ordenado?

2. Realizar el diagrama de Hasse correspondiente a la relación de inclusión entre los subconjuntos de $\{1, 2, 3\}$.

3. En $\mathbb{R}$ con el orden usual, considere el subconjuntos $A = \{\frac{1}{n}, \text{ con } n \in \mathbb{N}, \}$; $B = \{x \in \mathbb{R} \ : \ 1 \leq x < 2\}$; $C = \{x \in \mathbb{R} \ : \mid x \mid > 1\}$; y $D = (0, 1] \cup [2, 3]$.
   Determinar los elementos destacados (maximales, minimales, cotas, etc.) de cada uno de estos conjuntos.

4. Sea $A = \{x \in \mathbb{N} \ : \ 1 \leq x \leq 10\}$ y sean R y T dos relaciones de orden definidas en A dadas por

$$aRb \Longleftrightarrow a \text{ divide a } b;$$

$$aTb \Longleftrightarrow a \text{ es múltiplo de b.}$$

a) Hacer los diagrama de Hasse de las realciones R y T. En cada caso hallar los elementos maximales y los elementos minimales de A.

b) Lo mismo que en el inciso anterior pero en el conjunto $A - \{1\}$.

5. Demostrar que si a es primer elemento de un conjunto ordenado A entonces a es el único minimal de A. ♢

2.0.6. Relaciones de equivalencia

Una relación se dice **relación de equivalencia** si es reflexiva, simétrica y transitiva. Sea $\sim$ una relación de equivalencia en A y $a \in A$. Se llama **clase de equivalencia** de a (según la relación $\sim$) al conjunto que denotamos $\widetilde{a}$ formado por todos los elementos de A que están relacionados con a, es decir:

$$\widetilde{a} = \{x \in A : x \sim a\}.$$

El conjunto formado por las clases de equivalencias de los elementos de A se llama **conjunto cociente** de A por la relación $\sim$ y se denota $A/_{\sim}$; es decir:

$$A/_{\sim} = \{\widetilde{a} \text{ con } a \in A\}.$$

Observar que $A/_{\sim}$ es un conjunto cuyos elementos también son conjuntos.

Ejemplo 58.

1. La relación $=$ en un conjunto cualquiera es de equivalencia.
2. También es de equivalencia la relación $\parallel$ definida en el conjunto de rectas de un plano en la forma:
$$r \parallel l \leftrightarrow r \text{ es paralela a } l.$$
3. Sea B un subconjunto de un conjunto A. La relación $\sim$ definida en $\mathcal{P}(A)$ en la forma
$$X \sim Y \leftrightarrow X \cap B = Y \cap B,$$
es de equivalencia.
4. Es de equivalencia la relación en $\mathbb{R}$ dada por
$$x \sim y \leftrightarrow x - y \in \mathbb{Z}.$$

$\sim$ es reflexiva:

$$x \in \mathbb{R} \to x - x = 0 \to x - x \in \mathbb{Z} \to x \sim x.$$

$\sim$ es simétrica:

$$x \sim y \to x - y \in \mathbb{Z} \to -(x - y) \in \mathbb{Z} \to y - x \in \mathbb{Z} \to y \sim x.$$

$\sim$ es transitiva:

$$(x \sim y \ \wedge \ y \sim z) \to (x - y \in \mathbb{Z} \ \wedge \ y - z \in \mathbb{Z}) \to$$

$$\to (x - y) + (y - z) \in \mathbb{Z} \to x - z \in \mathbb{Z} \to x \sim z.$$

La clase de equivalencia de, por ejemplo, 0 es

$$\widetilde{0} = \{x \in \mathbb{R} : x \sim 0\} = \{x \in \mathbb{R} : x - 0 \in \mathbb{Z}\} = \{x \in \mathbb{R} : x \in \mathbb{Z}\} = \mathbb{Z}.$$

La clase de equivalencia de $\sqrt{2}$ es

$$\widetilde{\sqrt{2}} = \{x \in \mathbb{R} : x \sim \sqrt{2}\} = \{x \in \mathbb{R} : x - \sqrt{2} \in \mathbb{Z}\} =$$

$$= \{x : x = \sqrt{2} + k \text{ con } k \in \mathbb{Z}\} = \{\cdots, \sqrt{2} - 2, \sqrt{2} - 1, \sqrt{2}, \sqrt{2} + 1, \sqrt{2} + 2, \cdots\}$$

5. Es de equivalencia la relación $\equiv_2$ en $\mathbb{Z}$ dada por

$$m \equiv_2 m' \leftrightarrow 2 \text{ divide a } m - m'.$$

Esta relación se llama **equivalencia módulo** 2. En el capítulo 4 sobre número enteros, probaremos la validez de las propiedades utilizadas precedentemente y, en la Sección 4.1.1, estudiaremos las congruencias módulo n, con $n \in \mathbb{N}$ cualquiera. $\diamondsuit$

Las siguientes dos proposiciones muestran que existe una correspondencia entre las relaciones de equivalencias que se pueden definir en un conjunto y las particiones de ese conjunto: dada una relación de equivalencia queda definida una partición, esta partición es propia de la relación de equivalencia (de ninguna otra relación de equivalencia obtengo la misma partición); y recíprocamente, dada una partición queda definida una relación de equivalencia, esta relación de equivalencia es propia de la partición (de ninguna otra partición obtengo la misma relación de equivalencia).

Proposición 59. *Sea $\sim$ una relación de equivalencia en un conjunto A. La familia de conjuntos que denotamos*

$$(F)_{F\in A/\sim}$$

cuyos miembros son los conjuntos pertenecientes a $A/_\sim$, es una partición de A que se llama ***partición asociada a la relación*** *$\sim$.*

Demostración: Observar que si $F \in A/\sim$ entonces existe $a \in A$ tal que $F = \widetilde{a}$; por lo tanto, cada miembro de la familia $(F)_{F\in A/\sim}$ es un un subconjunto no vacío de A. Asumamos que F' es un miembro de la familia tal que $F \cap F' \neq \emptyset$; veremos que $F = F'$. Sea $a' \in A$ tal que $F' = \widetilde{a'}$ y llamemos b a un elemento en $F \cap F'$; es claro que $b \sim a$ y $b \sim a'$.
Sea x un elemento cualquiera de $\widetilde{a} = F$.

$$\begin{array}{rlll}
x \in \widetilde{a} & \rightarrow & x \sim a & \text{por definición de clase de equivalencia} \\
& \rightarrow & (x \sim a \wedge b \sim a) & \text{por adjunción} \\
& \rightarrow & (x \sim a \wedge a \sim b) & \text{por simetría} \\
& \rightarrow & x \sim b & \text{por transitividad} \\
& \rightarrow & (x \sim b \wedge b \sim a') & \text{por adjunción} \\
& \rightarrow & x \sim a' & \text{por transitividad} \\
& \rightarrow & x \in \widetilde{a'} & \text{por definición de clase de equivalencia.}
\end{array}$$

Hemos probado que $\widetilde{a} \subset \widetilde{a'}$.
Análogamente se prueba que $\widetilde{a'} \subset \widetilde{a}$. Así tenemos que $\widetilde{a} = \widetilde{a'}$, es decir, $F = F'$.
Finalmente, veamos que la unión de los miembros de la familia es A. Por definición, cada miembro F de la familia es un subconjunto de A, luego que

$$\bigcup_{F\in A/\sim} F \subset A.$$

Recíprocamente, si a es un elemento cualquiera de A entonces $a \in \widetilde{a} \in A/_\sim$; resulta que

$$A \subset \bigcup_{F\in A/\sim} F.$$

Hemos probado que $\bigcup_{F\in A/\sim} F = A$. □

Proposición 60. *Sea $(P_i)_{i\in I}$ una partición de un conjunto A. La relación $\sim$ definida en A en la forma*

$$x \sim y \leftrightarrow \text{ existe } i \in I \text{ tal que } x \in P_i \text{ e } y \in P_i,$$

es una relación de equivalencia en A que se llama ***relación asociada a la partición*** *$(P_i)_{i\in I}$.*

Demostración: Llamemos $\mathcal{P}$ a la partición $(P_i)_{i\in I}$.
r) $\sim$ es reflexiva: si $a \in A$, como $\mathcal{P}$ es partición de A, existe $i \in I$ tal que $a \in P_i$, entonces, $a \sim a$ por definicón de $\sim$.
s) $\sim$ simétrica: si $a \sim a'$ entonces existe $i \in I$ tal que $a \in P_i$ y $a' \in P_i$; de donde, existe $i \in I$ tal que $a' \in P_i$ y $a \in P_i$; resulta $a' \sim a$.
t) $\sim$ transitiva: si $a \sim a'$ y $a' \sim a''$ entonces existen i y j en I tales que

$$(a \in P_i \wedge a' \in P_i) \wedge (a' \in P_j \wedge a'' \in P_j);$$

esto implica que $a' \in P_i \cap P_j$. Como $\mathcal{P}$ es una partición de A, debe ser $P_i = P_j$. Así tenemos que $a \in P_i$ y $a'' \in P_i$ o, equivalentemente, $a \sim a''$ como queríamos probar.
De $r), s)$ y $t)$ resulta que $\sim$ es una relación de equivalencia. □

Ejercicio 61.
Probar que si $\sim$ es la relación de equivalencia asociada a la partición $(P_i)_{i\in I}$, entonces la partición asociada a $\sim$ es la misma $(P_i)_{i\in I}$. ♢

2.0.7. Funciones

Una **función** de un conjunto A en un conjunto B es una relación $\mathcal{R}$ de A en B que a cada elemento de A le hace corresponder uno y sólo un elemento de B; es decir, para todo $a \in A$ existe un único $b \in B$ tal que $(a, b) \in \mathcal{R}$. En otras palabras, para todo $a \in A$, el conjunto imagen $\mathcal{R}(\{a\})$ contiene un único elemento.

Ejemplo 62.

- Sean $A = \{1, 2, 3\}$, $B = \{a, b, c, d\}$ y las relaciones de A en B:

$$\mathcal{R}_1 = \{(1, a); (2, a)\};$$

$$\mathcal{R}_2 = \{(1, a); (1, b); (2, a); (3, c)\};$$

$$\mathcal{R}_3 = \{(1, a); (2, a); (3, c)\};$$

$$\mathcal{R}_4 = \{(1, b); (2, a); (3, c)\};$$

$$\mathcal{R}_5 = \{(1, a); (2, a); (3, a)\}.$$

La relación $\mathcal{R}_1$ no es función porque al elemento 3 de A no le corresponde ningún elemento de B; $\mathcal{R}_1(\{3\}) = \emptyset$.

La relación $\mathcal{R}_2$ no es función porque al elemento 1 de A no le corresponde un único elemento de B; $\mathcal{R}_2(\{1\}) = \{a, b\}$.

Las restantes tres relaciones son funciones de A en B. ♢

Ejercicio 63.

Indicar si las siguientes relaciones son funciones:

1. R de $\mathbb{N}$ en $\mathbb{N}$ dada por $xRy \leftrightarrow x.y = 4$.
2. R de $\mathbb{N}$ en $\mathbb{N}$ dada por $xRy \leftrightarrow x - y = 1$.
3. $\sim$ de $\mathcal{P}(A)$ en $\mathcal{P}(A)$ dada por $X \sim Y \leftrightarrow X \cup Y = A$, donde A es un conjunto cualquiera. ♢

Es usual indicar a las funciones con letras minúsculas. La notación $f : A \to B$ dice que f es una función del conjunto A en el conjunto B. Si $a \in A$ entonces $f(a)$ denota la **imagen de** a por f, es decir $f(a)$ es el único elemento de B con el cual se relaciona a mediante f. De esta forma se puede escribir que la función f es la relación

$$\{(a, f(a)) \text{ con } a \in A\}.$$

Algunas funciones pueden ser dadas indicando la imágen de un elemento genérico o variable que toma valores en el conjunto de partida, como veremos en el siguiente ejemplo.

Ejemplo 64.

- La función $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = n^2 + 1$.
- La función $p_A : A \times B \to A$ dada por $p_A((a, b)) = a$ se llama **proyección** sobre A.
- La función $id_A : A \to A$ dada por $id_A(x) = x$ se llama **identidad** en A.

- Sea S un subconjunto de A. La función $h_S : \mathcal{P}(A) \to \mathcal{P}(A)$ dada por $h_S(X) = X \cap S$.
- Sea S un subconjunto de A. La función $\chi_S : A \to \{0,1\}$ dada por

$$\chi_S(x) = \begin{cases} 1 & \text{si } x \in S; \\ 0 & \text{si } x \notin S, \end{cases}$$

  se llama **función característica** del conjunto S.
- Sea S es un subconjunto de A. La función $f : S \to A$ dada por $f(x) = x$ se llama **función de inclusión** de S en A. ♢

Dado que las funciones son relaciones, los resultado y definiciones relativos a relaciones que vimos al comienzo de este capítulo son aplicables a las funciones. Si $f : A \to B$; $A' \subset A$ y $B' \subset B$, es fácil ver que

$Dom(f) = A$	**dominio** de f
$Img(f) = \{f(a) \text{ con } a \in A\}$	**imagen** de f
$f(A') = \{f(a) \text{ con } a \in A'\}$	**imagen** de A'
$f^{-1}(B') = \{x \in A : f(x) \in B'\}$	**imagen inversa** de B'

Ejemplo 65.
Si $f : \mathbb{R} \to \mathbb{R}$ es la función

$$f(x) = \begin{cases} 1 & \text{si } x < -4 \\ 7 & \text{si } x \geq -4 \end{cases}$$

entonces

$Dom f = \mathbb{R}$	$Img(f) = \{1, 7\}$
$f(\{x \in \mathbb{R} : x < -6\}) = \{1\}$	$f(\{x \in \mathbb{R} : 0 \leq x\}) = \{7\}$
$f(\{-5, 5\}) = \{1, 7\}$	
$f^{-1}(\{0\}) = \emptyset$	$f^{-1}(\{1\}) = \{x \in \mathbb{R} : x < 4\}$

♢

Proposición 66. *Sea $f : A \to B$; A' y A'' subconjuntos de A; B' y B'' subconjuntos de B .*

1. *Si $A' \subset A''$ entonces $f(A') \subset f(A'')$.*
2. *$f(A' \cup A'') = f(A') \cup f(A'')$ y $f(A' \cap A'') \subset f(A') \cap f(A'')$.*

3. *Si* $B' \subset B''$ *entonces* $f^{-1}(B') \subset f^{-1}(B'')$.
4. $f^{-1}(B' \cup B'') = f(B') \cup f(B'')$ *y* $f^{-1}(B' \cap B'') = f^{-1}(B') \cap f^{-1}(B'')$.

Demostración: Probaremos el item 2), los restantes quedan como ejercicios.
Sea b un elemento cualquiera de $f(A' \cup A'')$.

$$\begin{aligned} b \in f(A' \cup A'') &\rightarrow \text{ existe } x \in A' \cup A'' \text{ tal que } f(x) = b \\ &\rightarrow (\text{ existe } x \in A'/f(x) = b) \vee (\text{ existe } x \in A''/f(x) = b) \\ &\rightarrow b \in f(A') \vee b \in f(A'') \\ &\rightarrow b \in f(A') \cup f(A''). \end{aligned}$$

Resulta que

$$f(A' \cup A'') \subset f(A') \cup f(A''). \tag{2.7}$$

Por otra parte, por el item 1) de esta misma proposición, como $A' \subset A' \cup A''$ y $A'' \subset A' \cup A''$, obtenemos que $f(A') \subset f(A' \cup A'')$ y $f(A'') \subset f(A' \cup A'')$; de donde

$$f(A') \cup f(A'') \subset f(A' \cup A''). \tag{2.8}$$

Las inclusiones (2.7) y (2.8), prueban que $f(A' \cup A'') = f(A') \cup f(A'')$.
En forma análoga se pueba que $f(A' \cap A'') \subset f(A') \cap f(A'')$. El siguiente ejemplo muestra que, en general, en el caso de la intersección, la igualdad puede no verificarse.

□

Ejemplo 67.
Sea $f : \mathbb{R} \rightarrow \mathbb{R}$ dada por $f(x) = x^2$, $A' = \{x \in \mathbb{R} : x < 0\}$ y $A'' = \{x \in \mathbb{R} : x > 0\}$.
Entonces,

$$f(A') = \{x \in \mathbb{R} : x > 0\},$$

$$f(A'') = \{x \in \mathbb{R} : x > 0\},$$

$$f(A') \cap f(A'') = \{x \in \mathbb{R} : x > 0\} \text{ y}$$

$$f(A' \cap A'') = f(\emptyset) = \emptyset.$$

♢ Dos funciones $f : A \rightarrow B$ y $g : C \rightarrow D$ son **iguales** si y sólo si $A = C$, $B = D$, y $f(x) = g(x)$ para todo $x \in A$.

Ejemplo 68.

- La función $f : \mathbb{R} \rightarrow \mathbb{R}_{\geq 0}$ dada por $f(x) = x^2$ no es igual a la función $g : \mathbb{R} \rightarrow \mathbb{R}$ dada por $g(x) = x^2$.

- La función $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = \frac{x^4-1}{x^2+1}$ es igual a la función $g : \mathbb{R} \to \mathbb{R}$ dada por $g(x) = x^2 - 1$. ♢

Se dice que una función $f : A \to B$ es

- **inyectiva** si no hay dos elementos de A con la misma imagen, es decir: para todo x y para todo y, se verifica que

$$f(x) = f(y) \to x = y;$$

- **suryectiva** si todo elemento de B es imagen de algún elemento de A, es decir:

$$Img(f) = B;$$

- **biyectiva** si es inyectiva y suryectiva.

Ejemplo 69.

- $p_B : A \times B \to B$ dada por $p_B((a,b)) = b$ no es inyectiva, a menos que A tenga un único elemento; en cambio, siempre es suryectiva. ♢

Ejercicio 70.

Determinar subconjuntos A y B de $\mathbb{R}$, tan grandes como sea posible, para que $f(x) = \frac{1}{x}$ sea una función suryectiva (inyectiva) de A en B.

Lo mismo para $g(x) = \frac{1}{x-|x|}$, $h(x) = \frac{2x}{x^2-1}$, y $t(x) = 3x + 6$. ♢

Dadas funciones $f : A \to B$ y $g : B \to C$, se llama f **compuesta con** g a la función de A en C que se denota $g \circ f$, dada por

$$g \circ f(x) = g(f(x)).$$

Ejemplo 71.

- Si $f : \mathbb{R} \to \mathbb{R}$ está dada por $f(x) = x^2 + 1$; y $g : \mathbb{R} \to \mathbb{R}$ es la función $g(x) = x^3$, entonces

$$g \circ f(x) = g(f(x)) = g(x^2 + 1) = (x^2 + 1)^3 = x^6 + 3x^4 + 3x^2 + 1;$$

$$f \circ g(x) = f(g(x))) = f(x^3) = (x^3)^2 + 1 = x^6 + 1.$$



Proposición 72. *Sean $f : A \to B$; $g : B \to C$ y $h : C \to D$ funciones cualesquiera; vale que*

1. $h \circ (g \circ f) = (h \circ g) \circ f$ *la composición de funciones es asociativa.*
2. $f \circ id_A = f$ *y* $id_B \circ f = f$.
3. *Si f es inyectiva y g es inyectiva, entonces $g \circ f$ es inyectiva. Si f es suryectiva y g es suryectiva, entonces $g \circ f$ es suryectiva.*
4. *Si $g \circ f$ es inyectiva entonces f es inyectiva. Si $g \circ f$ es suryectiva entonces g es suryectiva.*

Demostración: Demostraremos 4), los restantes puntos quedan como ejercicios.
Asumamos que $g \circ f$ es inyectiva. Sean a y a' elementos cualesquiera de A tales que $f(a) = f(a')$.

$$\begin{aligned} f(a) = f(a') &\to g(f(a)) = g(f(a')) \\ &\to g \circ f(a) = g \circ f(a') \quad \text{por definición de composición} \\ &\to a = a' \quad \text{porque } g \circ f \text{ es inyectiva .} \end{aligned}$$

Hemos probado que f es inyectiva.
Asumamos que $g \circ f$ es suryectiva. Sea c un elemento cualquiera de C.
Como $g \circ f : A \to C$ es suryectiva y $c \in C$, existe $a \in A$ tal que $g \circ f(a) = c$.
Sea $b = f(a)$; es claro que $b \in B$. Obtenemos que

$$g(b) = g(f(a)) = g \circ f(a) = c.$$

Hemos probado que g es suryectiva. □

Una función $f : A \to B$ **admite inversa**, o es **inversible**, si existe una función $g : B \to A$ tal que $g \circ f = id_A$ y $f \circ g = id_B$. En tal caso, la función g es única, se llama **función inversa** de f, se denota f^{-1} y es la relación inversa de f.
Efectivamente, asumamos que existe otra función $h : B \to A$ tal que $h \circ f = id_A$ y $f \circ h = id_B$; veremos que $g = h$. Utilizando el punto 2. de la Proposición 72 obtenemos que

$$g = g \circ id_B = g \circ (f \circ h) = (g \circ f) \circ h = id_A \circ h = h.$$

Proposición 73. *Una función admite inversa si y sólo si es biyectiva.*

Demostración: Asumamos que una función $f : A \to B$ admite inversa $f^{-1} : B \to A$. Sean a y a' elementos cualesquiera de A tales que $f(a) = f(a')$.

$$f(a) = f(a') \to f^{-1}(f(a)) = f^{-1}(f(a')) \to f^{-1} \circ f(a) = f^{-1} \circ f(a') \to$$
$$\to id_A(a) = id_A(a') \to a = a'.$$

Hemos probado que f es inyectiva.
Sea b un elemento cualquiera de B y sea $a = f^{-1}(b)$. Observar que $a \in A$ pues $f^{-1} : B \to A$. Como $f(a) = f(f^{-1}(b)) = f \circ f^{-1}(b) = id_B(b) = b$; resulta que f es suryectiva.
Ahora asumamos que una función $f : A \to B$ es biyectiva. Sea la función $g : B \to A$ dada por $g(y) = x$ donde x es el único elemento de A tal que $f(x) = y$. Observar que tal x existe pues f es suryectiva, y es único porque f es inyectiva. Resulta que $f \circ g(y) = f(g(y)) = f(x) = y = id_B(y)$ para todo $y \in B$. También $g \circ f(x) = g(f(x)) = g(y) = x = id_A(x)$ para todo $x \in A$. Hemos probado que f admite inversa y que $g = f^{-1}$. □

Ejercicio 74.
Probar que

1. $Dom(f^{-1}) = Img(f)$ y $Img(f^{-1}) = Dom(f)$.
2. $(f^{-1})^{-1} = f$.
3. Si $f : A \to B$ admite inversa y $g : B \to C$ admite inversa, entonces $g \circ f : A \to C$ admite inversa y $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. ♢

2.0.8. Conjuntos coordinables

Sean A y B conjuntos cualesquiera. Diremos que A y B son **coordinables**, o bien que **el cardinal de** A **es igual al cardinal de** B, o bien que A **y** B **tienen igual cardinal**, si existe una función biyectiva de A en B. En tal caso, escribiremos $| A | = | B |$. Es natural y acertado pensar que dos conjuntos tienen igual cardinal si y sólo si tienen igual cantidad de elementos.

Proposición 75. *La relación entre conjuntos definida en la forma*

$$A \simeq B \leftrightarrow | A | = | B |$$

es de equivalencia.

Demostración: Dado un conjunto A cualquiera, $id_A : A \rightarrow A$ es una función biyectiva, por lo tanto $A \simeq A$. Esto prueba que $\simeq$ es reflexiva.
Si A y B son conjuntos cualesquiera tales que $A \simeq B$, entonces existe una función $f : A \rightarrow B$ biyectiva. Como f es biyectiva, admite inversa $f^{-1} : B \rightarrow A$ que también es biyectiva. Resulta que $B \simeq A$. Hemos probado que $\simeq$ es simétrica.
Si A, B y C son conjuntos cualesquiera tales que $A \simeq B \simeq C$, entonces existe una función $f : A \rightarrow B$ biyectiva y existe una función $g : B \rightarrow C$ biyectiva. Como la composición de funciones biyectiva es una función biyectiva, resulta que $g \circ f : A \rightarrow C$ es biyectiva, de donde $A \simeq C$. Concluimos que $\simeq$ es transitiva. □

Sea $n \in \mathbb{N}$. Llamamos $\mathbb{I}_n$ al **intervalo natural** entre 1 y n, es decir, al conjunto $\{x \in \mathbb{N} : 1 \leq x \leq n\}$.
Un conjunto A se dice **finito** (o finito numerable) **con cardinal** n si $\mid A \mid = \mid I_n \mid$. También, por simplicidad, suele notarse $\mid A \mid = n$. Por extensión se dice que el conjunto vacío es finito con cardinal 0.
Un conjunto se dice **infinito** si no es finito.
Un conjunto A se dice **infinito numerable** si $\mid A \mid = \mid \mathbb{N} \mid$. También suele notarse $\mid A \mid = \chi_0$ (aleph cero).

Escribiremos $\mid A \mid \leq \mid B \mid$, que se lee **el cardinal de A es menor o igual al cardinal de B** o **el cardinal de B es mayor o igual que el cardinal de A**, si existe una función inyectiva de A en B.
Observar que si $A \subset B$ entonces $\mid A \mid \leq \mid B \mid$, pues la función inclusión de A en B es inyectiva.

Ejercicio 76.
Sean A y B conjuntos cualesquiera, probar que

1. $\mid A \mid = \mid B \mid \;\rightarrow\; (\mid A \mid \leq \mid B \mid \;\wedge\; \mid B \mid \leq \mid A \mid)$.
2. $(\mid A \mid \leq \mid B \mid \;\wedge\; \mid B \mid \leq \mid C \mid) \;\rightarrow\; \mid A \mid \leq \mid C \mid$. ♢

La implicación recíproca del inciso 1 del ejercicio anterior es el siguiente teorema cuya demostración omitiremos.

Teorema 77 (Cantor-Bernstein). *Sean A y B conjuntos cualesquiera. Si $\mid A \mid \leq \mid B \mid$ y $\mid B \mid \leq \mid A \mid$, entonces $\mid A \mid = \mid B \mid$.*

Escribiremos $\mid A \mid < \mid B \mid$, que se lee **el cardinal de** A **es estrictamente menor que el cardinal de** B o **el cardinal de** B **es estrictamente mayor que el cardinal de** A, si

$$\mid A \mid \leq \mid B \mid \quad \wedge \quad \mid A \mid \neq \mid B \mid .$$

Observar que $\mid A \mid \neq \mid B \mid$ significa que no existe ninguna función biyectiva de A en B.

Ejercicio 78.

Probar que si S es un subconjunto propio de un conjunto finito A entonces se satisface que $\mid S \mid < \mid A \mid$. ♢

El siguiente resultado prueba que no existe un conjunto con cardinal mayor que el cardinal de cualquier otro conjunto.

Proposición 79. *Si A es un conjunto cualquiera entonces $\mid A \mid < \mid \mathcal{P}(A) \mid$.*

Demostración: Sea A un conjunto cualquiera. La función $h : A \to \mathcal{P}(A)$ dada por $h(x) = \{x\}$ es inyectiva, por lo tanto $\mid A \mid \leq \mid \mathcal{P}(A) \mid$. A continuación probaremos por el método del absurdo que $\mid A \mid \neq \mid \mathcal{P}(A) \mid$.

Si $\mid A \mid = \mid \mathcal{P}(A) \mid$ entonces existe una función $f : A \to \mathcal{P}(A)$ biyectiva. Observar que para cada $x \in A$, $f(x)$ es un conjunto; luego, tiene sentido la definición del siguiente subconjunto de A:

$$H = \{x \in A : x \notin f(x)\}.$$

Ahora, $H \in \mathcal{P}(A)$ y $f : A \to \mathcal{P}(A)$ suryectiva, implica que existe un elemento $a \in A$ tal que

$$f(a) = H.$$

Si $a \in H$ entonces $a \notin f(a)$ por definición de H; pero $f(a) = H$, luego, $a \notin H$. Resulta $a \in H$ y $a \notin H$, una contradicción que proviene de suponer $a \in H$. Concluimos que

$$a \notin H.$$

Ahora, como $a \notin H$, tenemos que $a \in f(a)$ por definición de H; pero $f(a) = H$, entonces $a \in H$. Resulta $a \notin H$ y $a \in H$, una contradicción que proviene de suponer la existencia de a, es decir, de suponer que f es suryectiva.

Hemos probado que no existe una función biyectiva de A en $\mathcal{P}(A)$. □

Ejercicio 80.

Sean $P = \{x \in \mathbb{N} : x \text{ es par}\}$, $I = \{x \in \mathbb{N} : x \text{ es impar}\}$, a y b números reales cualesquiera tales que $a < b$. Mostrar funciones que prueben las siguientes relaciones:

$$\mid P \mid = \mid I \mid = \mid \mathbb{N} \mid = \mid \mathbb{Z} \mid = \mid \mathbb{Q} \mid$$

$$\mid (a,b) \mid = \mid (a,b] \mid = \mid [a,b] \mid = \mid [0,1] \mid = \mid \mathbb{R}_{\geq 0} \mid = \mid \mathbb{R} \mid$$

Se sugiere analizar la biyectividad de las siguientes funciones:

1. $f : \mathbb{N} \to P$ dada por $f(n) = 2n$.
2. $f : \mathbb{N} \to I$ dada por $f(n) = 2n - 1$.
3. $f : \mathbb{Z} \to \mathbb{N}$ dada por $f(m) = \begin{cases} 2m, & \text{si } m > 0; \\ -2m+1, & \text{si } m \leq 0. \end{cases}$
4. Sea $a \in \mathbb{N}$ un elemento dado.
   $f : \mathbb{N} \to \mathbb{N} - \{a\}$ dada por $f(n) = \begin{cases} n, & \text{si } n < a; \\ n+1, & \text{si } n \geq a. \end{cases}$
5. Función logaritmo $\ln : \mathbb{R}_{>0} \to \mathbb{R}$.
6. Función exponencial $\exp : \mathbb{R} \to \mathbb{R}_{>0}$.
7. Función tangente $\tan : (-\frac{\pi}{2}, \frac{\pi}{2}) \to \mathbb{R}$.
8. $f : \mathbb{R}_{>0} \to (0,1]$ dada por $f(x) = \frac{1}{1+x^2}$.
9. Sean a, b, c, d reales cualesquiera tales que $a < b$ y $c < d$;
   $g : [a,b] \to [c,d]$ dada por $g(x) = \frac{(d-c)}{(b-a)}(x-a) + c$.
10. $f : [0,1] \to (0,1)$ dada por $f(x) = \begin{cases} \frac{1}{2}, & \text{si } x = 0; \\ \frac{1}{n+2}, & \text{si } x = \frac{1}{n} \quad n \in \mathbb{N} \\ x, & \text{en otro caso.} \end{cases}$ ♢

Es fácil ver que $\mathbb{Q}$ es un subconjunto propio de $\mathbb{R}$, por ejemplo, en el Capítulo 4 probaremos que $\sqrt{2} \notin \mathbb{Q}$. Sin embargo, esto no implica que $\mid Q \mid < \mid \mathbb{R} \mid$. Para probar que $\mid Q \mid < \mid \mathbb{R} \mid$ debe mostrarse que no existe una función biyectiva de $\mathbb{Q}$ en $\mathbb{R}$. Tal demostración no será incluida en este trabajo.

Capítulo 3

Números naturales. Conteo

3.1. Propiedades de los números reales

En el conjunto $\mathbb{R}$ de los números reales están definidas dos operaciones: la **suma** que se denota $+$, y el **producto** que se denota $.$; y una relación de orden total que llamamos **orden usual de los reales** y se denota $\leq$.
Asumimos como conocidas las siguientes propiedades de los números reales; x, y, z son variables que toman valores en $\mathbb{R}$.

- La suma y el producto son operaciones **asociativas**, es decir,

$$(\forall x)(\forall y)(\forall z) \qquad (x+y)+z = x+(y+x);$$
$$(\forall x)(\forall y)(\forall z) \qquad (x.y).z = x.(y.x).$$

- La suma y el producto son operaciones **conmutativas**, es decir,

$$(\forall x)(\forall y) \qquad x+y = y+x;$$
$$(\forall x)(\forall y) \qquad x.y = y.z.$$

- El número real 0 es el **neutro de la suma**, es decir,

$$(\forall x) \qquad x+0 = x;$$

  y el número real 1 es el **neutro del producto**,

$$(\forall x) \qquad x.1 = x.$$

- Todo número real admite un **opuesto según la suma**, es decir, dado un número real x cualquiera, existe otro número real, que se denota $-x$, tal que $x + (-x) = 0$.
- Todo número real no nulo (distinto de 0) admite un **inverso según el producto**, es decir, dado un número real x cualquiera, $x \neq 0$, existe otro número real, que se denota x^{-1}, tal que $x.x^{-1} = 1$.
- El producto es distributivo con respecto a la suma, es decir,

$$(\forall x)(\forall y)(\forall z) \qquad x.(y + z) = x.y + x.z.$$

- $(\forall x)(\forall y)(\forall z) \qquad (x \leq y \ \rightarrow \ x + z \leq y + z).$
- $(\forall x)(\forall y)(\forall z) \qquad ((x \leq y \ \wedge \ 0 \leq z) \ \rightarrow \ x.z \leq y.z).$

Convención: Para simplificar la notación, podemos escribir:

- $x - y$ en lugar de $x + (-y)$;
- $\frac{1}{x}$ en lugar de x^{-1};
- $\frac{x}{y}$ en lugar de $x.y^{-1}$;
- $x < y$ cuando $x \leq y$ y $x \neq y$.
- $y \geq x$ y $y > x$ en lugar de $x \leq y$ y $x < y$, respectivamente.

Utilizando las propiedades anteriores se pueden deducir varias otras propiedades de los números reales,

Ejemplo 81. El opuesto de un número real es único.

En otras palabras, dado $x \in \mathbb{R}$, por las propiedades anteriores sabemos que existe $-x \in \mathbb{R}$ tal que $x+(-x) = 0$; probaremos que $-x$ es el único número real que cumple esta condición. Efectivamente, supongamos $x' \in \mathbb{R}$ y $x + x' = 0$;

$$\begin{array}{lll} x + x' = 0 & \rightarrow \ -x + (x + x') = -x + 0 & -x \text{ existe por propiedades anteriores} \\ & \rightarrow \ (-x + x) + x' = -x & + \text{ es asociativa y } 0 \text{ neutro} \\ & \rightarrow \ 0 + x' = -x & \text{por definición de opuesto} \\ & \rightarrow \ x' = -x & \text{pues } 0 \text{ es neutro de } +. \end{array}$$

$\diamondsuit$

Ejemplo 82. Propiedad cancelativa: dados números reales cualesquiera x,y y z,

si $x + z = y + z$ entonces $x = y$.

Efectivamente,

$$\begin{aligned} x+z=y+z \quad &\to \quad (x+z)+(-z)=(y+z)+(-z) \\ &\to \quad x+(z+(-z))=y+(z+(-z)) \quad \text{por propiedad asociativa} \\ &\to \quad x+0=y+0 \quad \text{por definición de opuesto} \\ &\to \quad x=y \quad \text{pues 0 es neutro para +.} \end{aligned}$$

♢

Ejemplo 83. Para todo $x \in \mathbb{R}$ se satisface que $x.0 = 0$.
Efectivamente,

$$x.0 \quad = \quad x.0+0 \quad \text{pues 0 es neutro para la suma;}$$

por otra parte,

$$\begin{aligned} x.0 &= x.(0+0) \quad \text{pues 0 es neutro para la suma;} \\ &= x.0+x.0 \quad \text{por propiedad distributiva;} \end{aligned}$$

igualando ambas expresiones obtenemos

$$x.0+0=x.0+x.0;$$

de donde $0 = x.0$ por la propiedad cancelativa. ♢

Ejemplo 84. Para todo par de números reales x e y se satisface que $-(x.y) = x.(-y)$. Para demostrar la validez de este enunciado, por la unicidad del opuesto probada anteriormente, basta ver que

$$x.y+x.(-y)=0.$$

Efectivamente,

$$\begin{aligned} x.y+x.(-y) &= x.(y+(-y)) \quad \text{por propiedad distributiva} \\ &= x.0 \quad \text{por definición de opuesto} \\ &= 0 \quad \text{por lo probado en el ejemplo anterior.} \end{aligned}$$

Ejercicio 85. Utilizando las propiedades anteriores, probar que se satisfacen las siguientes proposiciones para todo x, y, z en $\mathbb{R}$.

1. $(-x).y = x.(-y) = -(x.y)$
2. $(-x).(-y) = x.y$

3. $(x+y).(x-y) = x.x - y.y$
4. $x.y = 0 \longleftrightarrow (x = 0 \vee y = 0)$
5. $x.x = 1 \longleftrightarrow (x = 1 \vee x = -1)$
6. $\frac{x}{y} + \frac{w}{z} = \frac{x.z + y.w}{y.z}$
7. $\frac{x}{y}.\frac{w}{z} = \frac{x.w}{y.z}$
8. $0 < 1$
9. $x < 0 \rightarrow -x > 0.$ ♢

El **módulo** de un número real x se denota $\mid x \mid$ y se define de la siguiente forma,

$$\mid x \mid = \begin{cases} x, & \text{si } x \geq 0; \\ -x, & \text{si } x < 0. \end{cases}$$

Ejercicio 86. Utilizando las propiedades anteriores, probar que se satisfacen las siguientes proposiciones para todo x, y, z en $\mathbb{R}$.

1. $\mid x.y \mid = \mid x \mid . \mid y \mid$.
2. $\mid x^{-1} \mid = \mid x \mid^{-1}$. ♢

Un subconjunto S de $\mathbb{R}$ se dice **inductivo** si satisface las siguientes propiedades,

- $1 \in S$, y
- $(\forall x)(x \in S \rightarrow x + 1 \in S)$.

Ejemplo 87.

- $\{x \in \mathbb{R} : 4 < x\}$ no es inductivo.
- $\{x \in \mathbb{R} : -5 < x\}$ es inductivo.
- $\{x \in \mathbb{R} : 0 < x < 8 \ \vee \ 10 < x\}$ no es inductivo.
- $\mathbb{R}$ es inductivo. ♢

Proposición 88. *Si $(S_i)_{i \in I}$ es una familia de subconjuntos inductivos de $\mathbb{R}$ entonces $\bigcap_{i \in I} S_i$ es también un subconjunto inductivo de $\mathbb{R}$.*

Demostración: Como cada S_i es inductivo, tenemos que $1 \in S_i$ para todo $i \in I$, de donde

$$1 \in \bigcap_{i \in I} S_i. \tag{3.1}$$

Sea x un elemento cualquiera de $\bigcap_{i \in I} S_i$.

$$\begin{array}{lll} x \in \bigcap_{i\in I} S_i & \to \quad x \in S_i \text{ para todo } i & \text{por definición de intersección} \\ & \to \quad x+1 \in S_i \text{ para todo } i & \text{pues cada } S_i \text{ es inductivo} \\ & \to \quad x+1 \in \bigcap_{i\in I} S_i & \text{por definición de intersección.} \end{array}$$

Resulta que

$$\text{si } x \in \bigcap_{i\in I} S_i \text{ entonces } x+1 \in \bigcap_{i\in I} S_i. \tag{3.2}$$

Las relaciones (3.1) y (3.2) implican que $\bigcap_{i\in I} S_i$ es inductivo. □

A continuación, y en los capítulos siguientes, estudiaremos algunas propiedades de los siguientes subconjuntos de los números reales y de las operaciones definidas en ellos:

- el conjunto $\mathbb{N}$ de los **números naturales**;
- el conjunto $\mathbb{Z}$ de los **números enteros**;
- el conjunto $\mathbb{Q}$ de los **números racionales o fraccionarios**;
- y el conjunto $\mathbb{I}$ de los **números irracionales**.

Observar que la relación de orden $\leq$ (menor o igual) definida en $\mathbb{R}$ induce en cada uno de estos subconjuntos una relación de orden que también se denota $\leq$.

3.2. Números naturales

Los **números naturales** son aquellos que se obtienen sumando una cantidad finita de unos:

$$1,\ \ 1+1=2,\ \ (1+1)+1=3,\ \ ((1+1)+1)+1=4,\ \ \cdots$$

Así tenemos que $\mathbb{N} = \{1, 2, 3, 4, \cdots\}$. Observar que, por la propia definición dada, el conjunto $\mathbb{N}$ es inductivo; además,

$$\text{si } n \in \mathbb{N} \text{ y } n \neq 1 \text{ entonces } n-1 \in \mathbb{N}. \tag{3.3}$$

3.2.1. Inducción y definiciones recursivas

Para comenzar a trabajar con los números naturales debemos aceptar como axioma a uno de los siguientes dos principios.

Principio de buena ordenación *La relación "menor o igual", denotada* $\leq$*, es un buen orden en el conjunto de los números naturales* $\mathbb{N}$*: todo subconjunto no vacío de* $\mathbb{N}$ *tiene primer elemento.*

Principio de inducción *El conjunto* $\mathbb{N}$ *es el menor subconjunto inductivo de* $\mathbb{R}$*: si* $S \subset \mathbb{N}$ *y* S *es inductivo, entonces* $S = \mathbb{N}$*.*

Si aceptamos el primero, podemos probar como teorema al segundo; y si aceptamos el segundo, podemos probar como teorema al primero. Por esto decimos que ambos principios son equivalentes; a continuación demostraremos este hecho.

Proposición 89. *El principio de buena ordenación y el principio de inducción son equivalentes.*

Demostración: Asumamos que todo subconjunto no vacío de $\mathbb{N}$ tiene primer elemento y veamos que vale el principio de inducción. Sea $S \subset \mathbb{N}$ inductivo y supongamos $S \neq \mathbb{N}$. Entonces $\mathbb{N} - S \neq \emptyset$ y, en consecuencia, tiene primer elemento. Llamemos a a dicho primer elemento, es claro que

$$a - 1 \neq \mathbb{N} - S. \tag{3.4}$$

Por otra parte, $a \neq 1$ pues $1 \notin \mathbb{N} - S$. Luego, por (3.3),

$$a - 1 \in \mathbb{N}. \tag{3.5}$$

Las proposiciones (3.4) y (3.5) implican que $a - 1 \in S$.
Como S es inductivo, $(a-1)+1 = a \in S$, lo cual contradice que a pertenece a $\mathbb{N} - S$.
Concluimos que $S = \mathbb{N}$.
Ahora asumamos que $\mathbb{N}$ no tiene subconjuntos propios inductivos y veamos que vale el principio de buena ordenación. Consideremos $S = \{x \in \mathbb{N}$: todo subconjunto de $\mathbb{N}$ que contiene algún elemento menor o igual que x tiene primer elemento $\}$. Observar que $1 \in S$ y además,

$$m \in S \rightarrow m + 1 \in S,$$

pues dado un subconjunto H cualquiera de $\mathbb{N}$ que contiene algún elemento menor o igual que $m + 1$, si este subconjunto H contiene también algún elemento menor o igual que m entonces H tiene primer elemento porque por hipótesis $m \in S$; y si el

subconjunto H no contiene un elemento menor o igual que m entonces $m+1$ es su primer elemento.
Resulta que S es inductivo; en consecuencia, por el principio de inducción, $S = \mathbb{N}$.
Concluimos que todo subconjunto no vacío de $\mathbb{N}$ tiene primer elemento. □
En base al principio de inducción enunciado precedentemente, se obtiene el siguiente método de demostración.

Proposición 90 (Método inductivo)**.** *Sea n una variable que toma valores en $\mathbb{N}$ y sea $p(n)$ una función proposicional en la variable n. Si probamos que $p(1)$ es verdadera y probamos que para todo natural k, $p(k)$ implica $p(k+1)$, entonces hemos probado que $p(n)$ es verdadera para todo natural n.*

Demostración: Asumamos que $p(1)$ es verdadera y que para todo natural k,

$$p(k) \to p(k+1);$$

veremos que en tal caso $p(n)$ es verdadera para todo $n \in \mathbb{N}$.
Llamemos $S = \{n \in \mathbb{N} : p(n)\}$. Claramente S es un subconjunto de $\mathbb{N}$. Además, por las hipótesis consideradas, S es inductivo. Resulta, por el principio de inducción, que $S = \mathbb{N}$; por lo tanto, $p(n)$ es verdadera para todo natural n. □

Ejemplo 91. Probar que la suma es una **operación cerrada** en $\mathbb{N}$, es decir, la suma de dos números naturales es un número natural.
Sea m un número natural cualquiera. Probaremos por inducción (sobre la variable n) que

$$m + n \in \mathbb{N} \text{ para todo natural } n.$$

Si $n = 1$, $m + n = m + 1 \in \mathbb{N}$ pues, $m \in \mathbb{N}$ y $\mathbb{N}$ es inductivo.
Sea k un natural cualquiera y asumamos que $m + k \in \mathbb{N}$, veremos que

$$m + (k+1) \in \mathbb{N}.$$

Efectivamente, $m+(k+1) = (m+k)+1 \in \mathbb{N}$ pues por hipótesis inductiva $m+k \in \mathbb{N}$ y $\mathbb{N}$ es inductivo.
Hemos probado que, para todo natural n, se verifica que $m + n \in \mathbb{N}$.
Como m es un natural cualquiera, resulta que la suma de dos naturales cualesquiera es un natural. ♢

Ejemplo 92. Probar que el producto es una operación cerrada en $\mathbb{N}$, es decir, probar que el producto de dos números naturales es un número natural.

Sea m un número natural cualquiera. Probaremos por inducción sobre n que $m.n \in \mathbb{N}$ para todo natural n.

Si $n = 1$, la proposición vale pues $m.n = m.1 = m \in \mathbb{N}$.

Sea k un natural cualquiera y asumamos que $m.k \in \mathbb{N}$, veremos que $m.(k+1) \in \mathbb{N}$.

Efectivamente, $m.(k+1) = m.k + m.1 = m.k + m \in \mathbb{N}$ pues por hipótesis inductiva $m.k \in \mathbb{N}$ y la suma es cerrada en $\mathbb{N}$.

Hemos probado inductivamente que $m.n \in \mathbb{N}$ para todo natural n.

Luego, $m.n \in \mathbb{N}$ para todo $m \in \mathbb{N}$ y para todo $n \in \mathbb{N}$. $\diamondsuit$

Ejemplo 93. Demostrar que $n.(n+1)$ es par (múltiplo de 2) para todo número natural n. Observar que en este caso $p(n)$ es "$n.(n+1)$ es par".

Cuando $n = 1$ la proposición es verdadera pues $1.(1+1) = 1.2 = 2$ es par.

Sea k un natural cualquiera, asumamos que $k.(k+1)$ es par, es decir, asumamos que existe $m \in \mathbb{N}$ tal que $k.(k+1) = 2.m$; veremos que $(k+1).((k+1)+1)$ es par.

Efectivamente,

$$\begin{array}{rcll} (k+1).((k+1)+1) & = & (k+1).(k+(1+1)) & \text{propiedad asociativa} \\ & = & (k+1).(k+2) & \\ & = & (k+1).k + (k+1).2 & \text{propiedad distributiva} \\ & = & 2.m + (k+1).2 & \text{hipótesis inductiva} \\ & = & 2.(m+(k+1)) & \text{propiedad distributiva.} \end{array}$$

Hemos probado inductivamente que $n.(n+1)$ es par para todo natural n. $\diamondsuit$

Proposición 94. *Si a y b son números naturales y $a < b$ entonces $b - a \in \mathbb{N}$.*

Demostración: Sea $S = \{n \in \mathbb{N} : 1 \leq n \leq a\} \cup \{a + n \text{ con } n \in \mathbb{N}\}$. Observar que S es un conjunto inductivo y que $S \subset \mathbb{N}$, luego $S = \mathbb{N}$ y, en consecuencia, $b \in S$. Como $a < b$ debe ser que $b \in \{a + n \text{ con } n \in \mathbb{N}\}$, por lo tanto existe $n_0 \in \mathbb{N}$ tal que $b = a + n_0$; resulta que $b - a = (a + n_0) - a = n_0 \in \mathbb{N}$ como queríamos probar. $\square$

Proposición 95. *Si $S \subset \mathbb{N}$ es no vacío y existe $n_0 \in \mathbb{N}$ cota superior de S, entonces S tiene último elemento.*

Demostración: Sea $T = \{x \in \mathbb{N} : x \text{ es cota superior de } S\}$. Por hipótesis, S es no vacío; luego, T tiene primer elemento, sea a. Veremos que $a \in S$ y, en consecuencia, a es el último elemento de S.

Si $a = 1$, es claro que $S = \{1\}$ y así $a \in S$, como queríamos probar.

Asumamos $a > 1$; luego, por (3.3), $a - 1 \in \mathbb{N}$ y $a - 1 \notin T$, de donde a no es cota superior de S. Resulta que existe $b \in S$ tal que $a-1 < b$, y así tenemos que $a < b+1$. Por otra parte, como a es cota superior de S y $b \in S$, tenemos $b \leq a$. De las dos desigualdades, concluimos que $b \leq a < b + 1$; luego, $a = b \in S$. □

La idea de sucesión involucra dos conceptos: una cantidad de elementos y un orden entre ellos. Observar que en las tres sucesiones siguientes, claramente distintas entre sí, los elementos utilizados son los mismos, lo que difiere es el orden en que se presentan.

$$2, 4, 6, 8, 10, 12, ...$$

$$4, 2, 8, 6, 12, 10, ...$$

$$2, 4, 2, 6, 2, 8, 2, 10, 2, 12, ...$$

La manera formal de dar una **sucesión de números reales** es mediante una función de $\mathbb{N}$ en $\mathbb{R}$, así, el elemento que es imagen de 1 aparece en el primer lugar de la sucesión; el elemento que es imagen de 2 aparece en el segundo lugar de la sucesión;...; el elemento que es imagen de n aparece en el lugar n-ésimo en la sucesión.

La primera de las sucesión presentadas anterioremente es la función

$$a : \mathbb{N} \to \mathbb{R} \qquad \text{dada por} \qquad a(n) = 2.n.$$

La segunda es la función

$$b : \mathbb{N} \to \mathbb{R} \qquad \text{dada por} \qquad b(n) = \begin{cases} 2.(n+1), & \text{si } n \text{ es impar,} \\ 2.(n-1), & \text{si } n \text{ par.} \end{cases}$$

Y la tercera es la función

$$c : \mathbb{N} \to \mathbb{R} \qquad \text{dada por} \qquad c(n) = \begin{cases} 2, & \text{si } n \text{ es impar,} \\ n+2, & \text{si } n \text{ par.} \end{cases}$$

En general, dada una sucesión $s : \mathbb{N} \to \mathbb{R}$, es usual escribir s_n en lugar de $s(n)$. El término n-ésimo, expresado en función de n, se llama **término general de la sucesión**.

Hay distintas maneras de referirse a una sucesión, puede decirse:

Sea la sucesión $(a_n)_{n\in\mathbb{N}}$ dada por $a_n = 2n + 1$; o

Sea la sucesión $(a_n)_{n\geq 1}$ dada por $a_n = 2n + 1$; o

Sea la sucesión cuyo término n-ésimo es $a_n = 2n + 1$.

En cualquier caso nos estamos refiriendo a la sucesión 3, 5, 7, 9, 11, 13, $\cdots$

Ejemplo 96.

- La sucesión $(s_n)_{n\in\mathbb{N}}$ con $s_n = n.(n + 1)$ es la sucesión 2, 6, 12, 20, 30, $\cdots$
- La sucesión con término general $b_n = n^2 - 1$ es la sucesión 0, 3, 8, 15, 24,$\cdots$
- La sucesión con término general $c_n = 1$ es la sucesión 1, 1, 1, 1, 1, $\cdots$
- El término general de la sucesión 1, 8, 27, 64, $\cdots$ es $t_n = n^3$. ♢

Una sucesión se dice **definida por recurrencia** o **definida inductivamente** cuando está dada mediante el valor explícito de los primeros términos, y cada uno de los restantes términos se define suponiendo definidos los anteriores.

Ejemplo 97.

- La sucesión 3, 5, 7, 9, 11, 13, $\cdots$ puede definirse inductivamente en la forma:

  $a_1 = 3,$

  $a_n = a_{n-1} + 2$ para todo $n \geq 2$.

- La sucesión definida inductivamente en la forma:

  $s_1 = -1,$

  $s_n = -2.s_{n-1}$ para $n \geq 2$,

  es la sucesión -1, 2, -4, 8, -16, $\cdots$

- La sucesión definida inductivamente en la forma:

  $t_1 = 1,$

  $t_2 = 4,$

  $t_n = t_{n-1}.t_{n-2}$ para $n \geq 3$,

  es la sucesión 1, 4, 4, 16, 64, $\cdots$

- Dada la sucesión definida recursivamente en la forma:

  $s_1 = 1,$

  $s_n = n + s_{n-1}$ para $n \geq 2$,

probar que $s_n = \frac{n.(n+1)}{2}$ para todo n.

Podemos demostrar lo pedido por inducción sobre n.

Si $n = 1$ la proposicón es verdadera pues $\frac{1.(1+1)}{2} = \frac{2}{2} = 1 = s_1$.

Sea k un natural cualquiera, asumamos que $s_k = \frac{k.(k+1)}{2}$, veremos que $s_{k+1} = \frac{(k+1).((k+1)+1)}{2}$.

Efectivamente,

$$\begin{aligned}
s_{k+1} &= (k+1) + s_{(k+1)-1} && \text{por definición de la sucesión} \\
&= (k+1) + s_k \\
&= (k+1) + \tfrac{k.(k+1)}{2} && \text{por hipótesis inductiva} \\
&= (k+1)(1 + \tfrac{k}{2}) && \text{por propiedad distributiva} \\
&= (k+1)(\tfrac{2+k}{2}) \\
&= \tfrac{(k+1).((k+1)+1)}{2}.
\end{aligned}$$

Hemos probado inductivamente que $s_n = \frac{n.(n+1)}{2}$ para todo natural n. ♢

Veremos a continuación otras definiciones dadas por recurrencia.

Potencia n-ésima: es sabido que si $a \in \mathbb{R}$ y $n \in \mathbb{N}$, la potencia n-ésima de a es el número real que se denota a^n y que se obtiene multiplicando a a por sí mismo n veces, es decir,

$$a^n = \underbrace{a.a.\cdots.a}_{n \text{ veces}}$$

Esta definición se puede formalizar dándola en forma recursiva:

$a^1 = a$,

$a^n = a.a^{n-1}$ para $n \geq 2$.

Factorial: Sea n un número natural cualquiera. Se define inductivamente el factorial de n, denotado $n!$, en la forma:

$1! = 1$,

$n! = (n-1)!.n$ para $n \geq 2$.

Veamos como se interpreta esta definión:

$1! = 1.$

$2! = 1!.2 = 1.2 = 2.$

$3! = 2!.3 = 1.2.3 = 6.$

$4! = 3!.4 = 1.2.3.4 = 24.$

$\vdots$

$n! = 1.2.3.\cdots.n.$

Por extensión se define $0! = 1$.

Sumatoria: Sea $(a_n)_{n\in\mathbb{N}}$ una sucesión de números reales y m un número natural. La sumatoria de los m primero términos de la sucesión, que se denota $\sum_{n=1}^{m} a_n$ (se lee " sumatoria desde $n = 1$ hasta m de a_n"), se define inductivamente en la forma:

$\sum_{n=1}^{1} a_n = a_1,$

$\sum_{n=1}^{m} a_n = (\sum_{n=1}^{m-1} a_n) + a_m \quad \text{para } m \geq 2.$

Como en el caso anterior es fácil interpretar que

$\sum_{n=1}^{m} a_n = a_1 + a_2 + a_3 + \cdots + a_m.$

Observar que, por ejemplo,

$\sum_{n=1}^{m} 2.n = 2.1 + 2.2 + 2.3 + \cdots + 2.m.$

$\sum_{n=1}^{m} n^3 = 1^3 + 2^3 + 3^3 + \cdots + m^3.$

$\sum_{n=1}^{m} 4^n = 4^1 + 4^2 + 4^3 + \cdots + 4^m.$

$\sum_{n=1}^{m} 5 = 5 + 5 + 5 + 5 \cdots + 5 = m.5.$

Para k y m números naturales con $k \leq m$, se define

$\sum_{n=k}^{m} a_n = (\sum_{n=1}^{m} a_n) - (\sum_{n=1}^{k-1} a_n).$

Productoria: Sea (a_n) una sucesión de números reales y m un número natural dado cualquiera. El producto de los m primero términos de la sucesión, denotada por $\prod_{n=1}^{m} a_n$ (se lee " productoria desde $n = 1$ hasta m de a_n), se define inductivamente en la forma:

$\prod_{n=1}^{1} a_n = a_1$,

$\prod_{n=1}^{m} a_n = (\prod_{n=1}^{m-1} a_n).a_m \quad$ para $m \geq 2$.

Ejemplo 98. Probar que $\sum_{n=1}^{m} n = \frac{m.(m+1)}{2}$ para todo natural m.
Esta fórmula nos dice que, por ejemplo, para $m = 4$,

$$\sum_{n=1}^{4} n = 1 + 2 + 3 + 4 = \frac{4.5}{2} = 10;$$

para $m = 100$,

$$\sum_{n=1}^{100} n = 1 + 2 + 3 + \cdots + 100 = \frac{100.101}{2} = 550.$$

Para demostrar que la fórmula vale para todo $m \in \mathbb{N}$, procederemos por inducción en m.
Si $m = 1$, la proposición es verdadera pues $\sum_{n=1}^{m} n = \sum_{n=1}^{1} n = 1$ y $\frac{m.(m+1)}{2} = \frac{1.(1+1)}{2} = 1$.
Sea k un natural cualquiera y asumamos que $\sum_{n=1}^{k} n = \frac{k.(k+1)}{2}$; veremos que $\sum_{n=1}^{k+1} n = \frac{(k+1).((k+1)+1)}{2}$.
Efectivamente,

$$\begin{aligned}
\sum_{n=1}^{k+1} n &= (\sum_{n=1}^{k} n) + (k+1) && \text{por definición de sumatoria} \\
&= \frac{k.(k+1)}{2} + (k+1) && \text{por hopótesis inductiva} \\
&= (k+1).(\frac{k}{2} + 1) && \text{propiedad distributiva} \\
&= \frac{(k+1).((k+1)+1)}{2}.
\end{aligned}$$

Hemos probado inductivamente que $\sum_{n=1}^{m} n = \frac{m.(m+1)}{2}$ para todo natural m. ♢
Las siguientes dos proposiciones nos ofrecen formas alternativas de uso del método de demostración por inducción. Omitiremos las pruebas de estas proposiciones pues cada una de ellas es muy similar a la prueba de la Proposición 3.2.

Proposición 99 (Generalización del método inductivo)**.** *Sea n una variable que toma valores en $\mathbb{N}$, sea $p(n)$ una función proposicional en la variable n, y sea n_0 un número natural cualquiera. Si probamos que $p(n_0)$ es verdadera y probamos que*

para todo natural $k \geq n_0$, $p(k)$ implica $p(k+1)$, entonces hemos probado que $p(n)$ es verdadera para todo natural $n \geq n_0$.

Ejemplo 100. Probar que $2^n < n!$ para todo natural $n \geq 4$.
Para $n = 4$ la proposición es válida pues $2^n = 2^4 = 16$, $n! = 4! = 1.2.3.4 = 24$ y $16 < 24$.
Sea k un natural cualquiera, $k \geq 4$, y asumamos que $2^k < k!$, veremos que $2^{k+1} < (k+1)!$.
Efectivamente,

$$\begin{aligned} 2^{k+1} &= 2^k.2 && \text{por definición de potencia} \\ &< k!.2 && \text{por hipótesis inductiva} \\ &< k!.(k+1) && \text{pues } 2 < k+1 \\ &= (k+1)! && \text{por definición de factorial.} \end{aligned}$$

Hemos probado inductivamente que $2^n < n!$ para todo natural $n \geq 4$. ♢

Proposición 101 (Método inductivo fuerte). *Sea n una variable que toma valores en $\mathbb{N}$ y sea $p(n)$ una función proposicional en la variable n. Si probamos que $p(1)$ es verdadera y probamos que para todo natural k, la validez de $p(m)$ para todo $m \leq k$ implica $p(k+1)$, entonces hemos probado que $p(n)$ es verdadera para todo natural n.*

Ejemplo 102. Probar que la sucesión $(a_n)_{n\in\mathbb{N}}$ definida inductivamente en la forma $a_1 = 8$, $a_2 = 34$ y $a_n = 8.a_{n-1} - 15.a_{n-2}$ para $n \geq 3$; y la sucesión $(b_n)_{n\in\mathbb{N}}$ con término general $b_n = 3^n + 5^n$, son iguales.
Debemos probar que,

$a_n = b_n$ para todo natural n.

Utilizaremos el principio de inducción fuerte.
Si $n = 1$, la proposición es válida pues $a_1 = 8$ y $b_1 = 3^1 + 5^1 = 3 + 5 = 8$.
Sea k un natural cualquiera y asumamos que para todo $m \leq k$ se cumple que $a_m = b_m$, veremos que $a_{k+1} = b_{k+1}$. Efectivamente, (deberé considerar dos casos pues la definición de a_{k+1} varía según sea $k+1 = 2$ o $k+1 > 2$)

- si $k+1 = 2$, entonces $a_{k+1} = a_2 = 34$ y $b_{k+1} = b_2 = 3^2 + 5^2 = 9 + 25 = 34$.
- si $k+1 \geq 3$, entonces

$$\begin{aligned}
a_{k+1} &= 8.a_{(k+1)-1} - 15.a_{(k+1)-2} && \text{por definición} \\
&= 8.a_k - 15.a_{k-1} \\
&= 8.(3^k + 5^k) - 15.a_{k-1} && \text{hipótesis inductiva para } a_k \\
&= 8.(3^k + 5^k) - 15.(3^{k-1} + 5^{k-1}) && \text{hipótesis inductiva para } a_{k-1} \\
&= 8.(3^k + 5^k) - (3.5.3^{k-1} + 3.5.5^{k-1}) && \text{distributiva y } 15 = 3.5 \\
&= 8.(3^k + 5^k) - (5.3^k + 3.5^k) \\
&= 3^k.(8-5) + 5^k.(8-3) \\
&= 3^{k+1} + 5^{k+1} \\
&= b_{k+1} && \text{por definición.}
\end{aligned}$$

Hemos probado inductivamente que $a_n = b_n$ para todo natural n. ♢

Ejercicio 103. Probar la validez de los siguientes enunciados.

1. Propiedades de la potenciación: para a y b números reales cualesquiera, y n y m números naturales cualesquiera, se satisface que,
   - $(a.b)^n = a^n.b^n$
   - $(\frac{a}{b})^n = \frac{a^n}{b^n}$
   - $a^n.a^m = a^{n+m}$
   - $(a^n)^m = a^{n.m}$
2. Propiedades de la sumatoria: para $(a_n)_{n\in\mathbb{N}}$ y $(b_n)_{n\in\mathbb{N}}$ sucesiones cualesquiera de números reales, $c \in \mathbb{R}$ y $m \in \mathbb{N}$ vale que,
   - $(\sum_{n=1}^m a_n) + (\sum_{n=1}^m b_n) = \sum_{n=1}^m (a_n + b_n)$.
   - $c.(\sum_{n=1}^m a_n) = \sum_{n=1}^m (c.a_n)$.
3. $n < 2^n$ para todo natural n.
4. Para todo natural n, $\sum_{n=1}^m 2^n = 2.(2^m - 1)$.
5. Probar que para todo $n \geq 4$ se satisface que $3^n - 2^n > n^3$.
6. Probar que si $a_n = 1$, $a_2 = 3$ y $a_n = a_{n-1} + 5.a_{n-2}$ para todo $n \geq 3$, entonces $a_n < 1 + 3^{n-1}$ para todo natural n.
7. Sea a un número real cualquiera, probar que

$$\sum_{n=10}^{15} a^n\,(3.n-2) = \sum_{n=1}^{6} a^{n+9}\,(3.(n+9)-2).$$

8. Sea $(b_n)_{n\in\mathbb{N}}$ una sucesión de números reales, probar que para r y s cualesquiera con $r \leq s$, vale que
$$\sum_{n=r}^{s} b_n = \sum_{n=1}^{s-r+1} b_{n+r-1}.$$



3.2.2. Números Combinatorios y Binomio de Newton

Llamaremos $\mathbb{N}_0$ al conjunto $\mathbb{N} \cup \{0\}$. Dados n y m en $\mathbb{N}_0$, con $m \leq n$, se define el **número combinatorio** n m, denotado $\begin{pmatrix} n \\ m \end{pmatrix}$, en la forma:
$$\begin{pmatrix} n \\ m \end{pmatrix} = \frac{n!}{(n-m)!\,m!}$$

Ejemplo 104.
$$\begin{pmatrix} 8 \\ 3 \end{pmatrix} = \tfrac{8!}{(8-3)!\,3!} = \tfrac{8!}{5!\,3!} = \tfrac{8.7.6}{3.2} = 56.$$

Ejemplo 105. Si $n \in \mathbb{N}$,
$$\begin{pmatrix} n \\ 0 \end{pmatrix} = \tfrac{n!}{(n-0)!\,0!} = \tfrac{n!}{n!} = 1;$$
$$\begin{pmatrix} n \\ 1 \end{pmatrix} = \tfrac{n!}{(n-1)!\,1!} = n;$$
$$\begin{pmatrix} n \\ n-1 \end{pmatrix} = \tfrac{n!}{(n-(n-1))!\,(n-1)!} = \tfrac{n!}{(n-1)!} = n;$$
$$\begin{pmatrix} n \\ n \end{pmatrix} = \tfrac{n!}{(n-n)!\,n!} = \tfrac{n!}{n!} = 1.$$



Proposición 106. *Para todo par de números n y m en $\mathbb{N}_0$, con $m \leq n$, se verifica que:*

1. $\begin{pmatrix} n \\ m \end{pmatrix} = \begin{pmatrix} n \\ n-m \end{pmatrix}.$

2. $\begin{pmatrix} n \\ m \end{pmatrix} = \begin{pmatrix} n-1 \\ m \end{pmatrix} + \begin{pmatrix} n-1 \\ m-1 \end{pmatrix}$ *siempre que* $n > m \geq 1$.

3. $\begin{pmatrix} n \\ m \end{pmatrix} \in \mathbb{N}$.

Demostración: 1. Por definición tenemos que

$$\begin{pmatrix} n \\ n-m \end{pmatrix} = \frac{n!}{(n-(n-m))!.(n-m)!} = \frac{n!}{m!.(n-m)!} = \begin{pmatrix} n \\ m \end{pmatrix}.$$

2. Por definición tenemos que

$$\begin{pmatrix} n-1 \\ m \end{pmatrix} + \begin{pmatrix} n-1 \\ m-1 \end{pmatrix} = \frac{(n-1)!}{((n-1)-m)!.m!} + \frac{(n-1)!}{((n-1)-(m-1))!.(m-1)!} =$$

$$= \frac{(n-1)!}{(n-m-1)!.m!} + \frac{(n-1)!}{(n-m)!.(m-1)!} = \frac{(n-1)!}{(n-m-1)!.(m-1)!}.(\frac{1}{m} + \frac{1}{(n-m)}) =$$

$$= \frac{(n-1)!}{(n-m-1)!.(m-1)!}.(\frac{(n-m)+m}{m.(n-m)}) = \frac{(n-1)!}{(n-m-1)!.(m-1)!}.\frac{n}{m.(n-m)} =$$

$$= \frac{n!}{(n-m)!.m!} = \begin{pmatrix} n \\ m \end{pmatrix}.$$

3. Si $n = 0$ o $m = 0$, es fácil ver que la proposición es verdadera. Asumamos entonces que n y m son naturales. Probaremos por inducción en n que:

para todo natural $m \leq n$ se verifica que $\begin{pmatrix} n \\ m \end{pmatrix} \in \mathbb{N}$.

Si $n = 1$ la proposición es verdadera pues en este caso debe ser $m = 1$ y

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1 \in \mathbb{N}.$$

Sea k un natural cualquiera y asumamos que la proposición vale para k, es decir, asumamos que

para todo natural $m \leq k$ se verifica que $\begin{pmatrix} k \\ m \end{pmatrix} \in \mathbb{N}$;

veremos que la proposición vale para $k+1$, es decir, veremos que

para todo natural $m \leq k+1$ se verifica que $\begin{pmatrix} k+1 \\ m \end{pmatrix} \in \mathbb{N}$.

.

Efectivamente, sea h un natural cualquiera con $h \leq k+1$,

- si $h = k+1$ entonces $\begin{pmatrix} k+1 \\ h \end{pmatrix} = \begin{pmatrix} k+1 \\ k+1 \end{pmatrix} = 1 \in \mathbb{N}$.
- si $h < k+1$, por el segundo inciso de esta misma proposición, tenemos que

$$\begin{pmatrix} k+1 \\ h \end{pmatrix} = \begin{pmatrix} k \\ h \end{pmatrix} + \begin{pmatrix} k \\ h-1 \end{pmatrix}.$$

Por hipótesis inductiva ambos números, $\begin{pmatrix} k \\ h \end{pmatrix}$ y $\begin{pmatrix} k \\ h-1 \end{pmatrix}$ son naturales pues $h-1 \leq k$ y $h \leq k$. Como la suma es cerrada en $\mathbb{N}$, resulta que $\begin{pmatrix} k+1 \\ h \end{pmatrix} \in \mathbb{N}$.

Hemos probado inductivamente que para todo natural n y todo natural $m \leq n$ se verifica que $\begin{pmatrix} n \\ m \end{pmatrix} \in \mathbb{N}$. □

La siguiente disposición de los números combinatorios es conocida como **Triángulo de Pascal** o **Triángulo de Tartaglia**.

$$\begin{array}{ccccccccc}
 & & \begin{pmatrix} 1 \\ 0 \end{pmatrix} & & \begin{pmatrix} 1 \\ 1 \end{pmatrix} & & & & \\
 & \begin{pmatrix} 2 \\ 0 \end{pmatrix} & & \begin{pmatrix} 2 \\ 1 \end{pmatrix} & & \begin{pmatrix} 2 \\ 2 \end{pmatrix} & & & \\
\begin{pmatrix} 3 \\ 0 \end{pmatrix} & & \begin{pmatrix} 3 \\ 1 \end{pmatrix} & & \begin{pmatrix} 3 \\ 2 \end{pmatrix} & & \begin{pmatrix} 3 \\ 3 \end{pmatrix} & & \\
\begin{pmatrix} 4 \\ 0 \end{pmatrix} & \begin{pmatrix} 4 \\ 1 \end{pmatrix} & & \begin{pmatrix} 4 \\ 2 \end{pmatrix} & & \begin{pmatrix} 4 \\ 3 \end{pmatrix} & & \begin{pmatrix} 4 \\ 4 \end{pmatrix} & \\
\vdots & & \vdots & & \vdots & & & \vdots &
\end{array}$$

Observar que los números que aparecen en los extremos de cada fila son iguales a 1; en tanto que cualquier otro, por lo probado en el item 2 de la Proposición 106, es la suma de los dos superiores. Tenemos, entonces, que dicho triangulo es:

$$\begin{array}{ccccccccccc} & & & & 1 & & 1 & & & & \\ & & & 1 & & 2 & & 1 & & & \\ & & 1 & & 3 & & 3 & & 1 & & \\ & 1 & & 4 & & 6 & & 4 & & 1 & \\ 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\ \vdots & & & & & \vdots & & & & & \vdots \end{array}$$

Veremos en la siguiente proposición que los números que aparecen en la fila n-ésima de este triángulo corresponden a los coeficientes que aparecen en el desarrollo de la potencia n-ésima de un binomio, es decir:

$$\begin{aligned} (a+b)^1 &= a+b; \\ (a+b)^2 &= a^2+2.a.b+b^2; \\ (a+b)^3 &= a^3+3.a^2.b+3.a.b^2+b^3; \\ (a+b)^4 &= a^4+4.a^3.b+6.a^2.b^2+4.a.b^3+b^4; \\ \vdots & \quad \vdots \end{aligned}$$

Proposición **107** (Binomio de Newton)**.** *Si a y b son número reales y $n \in \mathbb{N}$, entonces*

$$(a+b)^n = \sum_{i=0}^{n} \begin{pmatrix} n \\ i \end{pmatrix} a^i\, b^{n-i}.$$

Demostración: Procederemos por inducción en $\mathbb{N}$.
Si $n = 1$, $(a+b)^1 = a+b$ y, por otra parte,
$\sum_{i=0}^{1} \begin{pmatrix} n \\ i \end{pmatrix} a^i\, b^{n-i} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} a^0\, b^{1-0} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} a^1\, b^{1-1} = b+a = a+b$,
por lo tanto la proposición es verdadera.
Sea k un natural cualquiera y asumamos que $(a+b)^k = \sum_{i=0}^{k} \begin{pmatrix} k \\ i \end{pmatrix} a^i\, b^{k-i}$.
Entonces, usando la hipótesis inductiva, tenemos que
$(a+b)^{k+1} = (a+b)^k.(a+b) = (\sum_{i=0}^{k} \begin{pmatrix} k \\ i \end{pmatrix} a^i\, b^{k-i}).(a+b) =$
$= (\sum_{i=0}^{k} \begin{pmatrix} k \\ i \end{pmatrix} a^i\, b^{k-i}).a + (\sum_{i=0}^{k} \begin{pmatrix} k \\ i \end{pmatrix} a^i\, b^{k-i}).b =$

$= (\sum_{i=0}^{k} \begin{pmatrix} k \\ i \end{pmatrix} a^{i+1}\, b^{k-i}) + (\sum_{i=0}^{k} \begin{pmatrix} k \\ i \end{pmatrix} a^{i}\, b^{k-i+1}) =$

$= (\sum_{i=0}^{k-1} \begin{pmatrix} k \\ i \end{pmatrix} a^{i+1}\, b^{k-i}) + \begin{pmatrix} k \\ k \end{pmatrix} a^{k+1}\, b^{0} + \begin{pmatrix} k \\ 0 \end{pmatrix} a^{0}\, b^{k-0+1} +$

$+ (\sum_{i=1}^{k} \begin{pmatrix} k \\ i \end{pmatrix} a^{i}\, b^{k-i+1}) = (*)$

Observando que

$\sum_{i=0}^{k-1} \begin{pmatrix} k \\ i \end{pmatrix} a^{i+1}\, b^{k-i} = \sum_{i=1}^{k} \begin{pmatrix} k \\ i-1 \end{pmatrix} a^{i}\, b^{k-i+1};$

y reordenando los términos, obtenemos

$(*) = \begin{pmatrix} k \\ 0 \end{pmatrix} a^{0}\, b^{k+1} + (\sum_{i=1}^{k} \begin{pmatrix} k \\ i-1 \end{pmatrix} a^{i}\, b^{k-i+1}) +$

$+ (\sum_{i=1}^{k} \begin{pmatrix} k \\ i \end{pmatrix} a^{i}\, b^{k-i+1}) + \begin{pmatrix} k \\ k \end{pmatrix} a^{k+1}\, b^{0} = (**)$

Uniendo ambas sumatorias, resulta

$(**) = \begin{pmatrix} k \\ 0 \end{pmatrix} a^{0}\, b^{k+1} + \sum_{i=1}^{k} (\begin{pmatrix} k \\ i-1 \end{pmatrix} + \begin{pmatrix} k \\ i \end{pmatrix}) a^{i}\, b^{k-i+1} +$

$+ \begin{pmatrix} k \\ k \end{pmatrix} a^{k+1}\, b^{0} = (***)$

Observando que

$\begin{pmatrix} k \\ 0 \end{pmatrix} = \begin{pmatrix} k+1 \\ 0 \end{pmatrix}; \quad \begin{pmatrix} k \\ i-1 \end{pmatrix} + \begin{pmatrix} k \\ i \end{pmatrix} = \begin{pmatrix} k+1 \\ i \end{pmatrix}; \quad \begin{pmatrix} k \\ k \end{pmatrix} = \begin{pmatrix} k+1 \\ k+1 \end{pmatrix},$

concluimos

$(***) = \begin{pmatrix} k+1 \\ 0 \end{pmatrix} a^{0}\, b^{k+1} + (\sum_{i=1}^{k} \begin{pmatrix} k+1 \\ i \end{pmatrix} a^{i}\, b^{k-i+1}) + \begin{pmatrix} k+1 \\ k+1 \end{pmatrix} a^{k+1}\, b^{0} =$

$= \sum_{i=0}^{k+1} \begin{pmatrix} k+1 \\ i \end{pmatrix} a^{i}\, b^{(k+1)-i}$; lo cual completa la prueba inductiva. □

3.3. Conteo

Veremos como resolver algunos problemas en los cuales se plantea la necesidad de determinar la cantidad de formas en que se puede realizar alguna tarea.

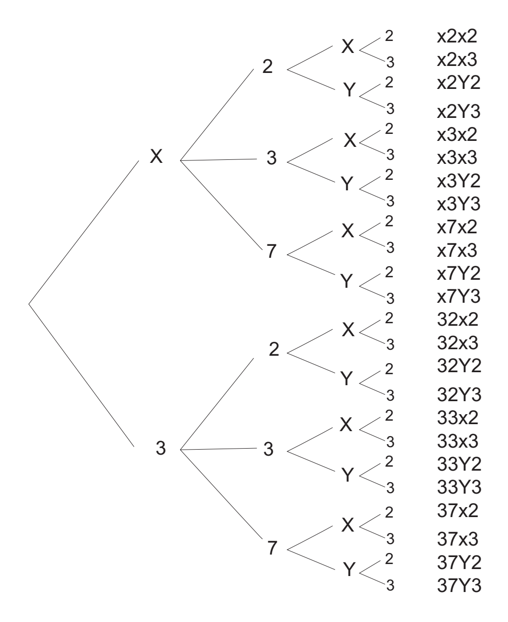


Figura 3.1: diagrama de árbol: la primer columna se corresponde con el primer caracter del código (puede ser x o 3); la segunda con el segundo caracter (puede ser 2, 3 o 7), la tercera con el tercer caracter (puede ser x o y) y la cuarta con el cuarto caracter (puede ser 2 o 3). En la quinta columna aparecen listados los códigos resultantes.

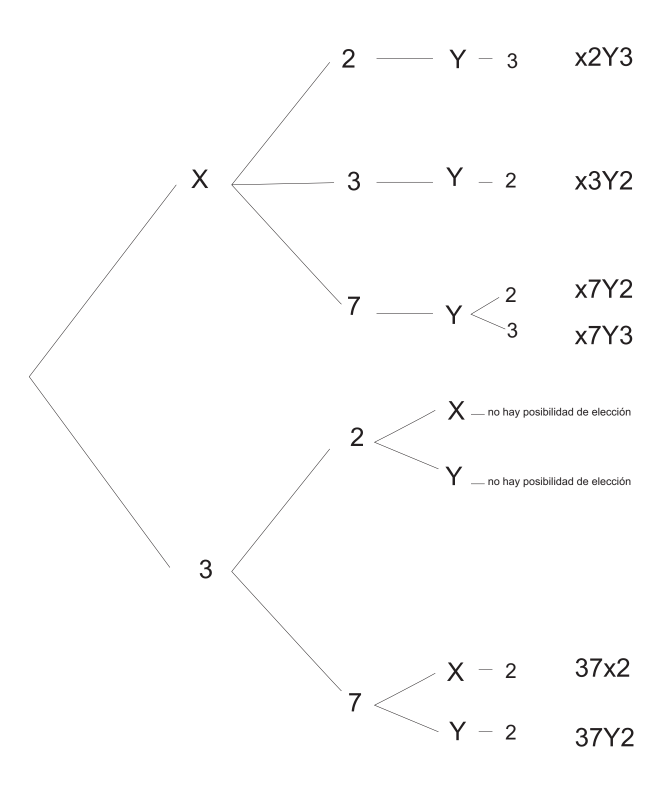


Figura 3.2: diagrama de árbol: como no puedo repetir símbolos, cada elección se ve limitada por lo que haya elegido antes.

Ejemplo 108.

- ¿De cuántas formas pueden ordenarse en una fila 3 personas? Respuesta: de 6 formas distintas; si llamamos respectivamente A, B y C a las tres personas, tenemos que las formas en que pueden ordenarse son:

  A-B-C A-C-B B-A-C B-C-A C-A-B C-B-A

  ¿Y si en lugar de 3 pesonas tenemos 50 personas o 100 personas?¿Hay una fórmula general que da respuesta a esta pregunta? ¿Y si en lugar de ordenar personas en una fila se trata de ordenar libros en un estante?
- Se debe crear un código de seguridad con cuatro caracteres siguiendo la siguiente regla: el primer caracter (leyendo de izquierda a derecha) puede ser x o 3; el segundo caracter puede ser 2, 3 o 7; el tercer caracter puede ser x o y; y el cuarto puede ser 2 o 3.

  ¿De cuántas formas puede hacerse? Rta: de 24 formas distintas; para representarlas utilizamos un esquema que se llama **árbol de decisión** o **diagrama de árbol**, el cual describimos en la Figura 3.1. Al final de cada línea del árbol escribimos el código que surge de la misma.

  Ahora nos preguntamos: ¿cuántos códigos distintos se pueden formar si agregamos la restricción de no permitir repetición de símbolos? Rta: en este caso, también mediante el diagrama de árbol descripto en la Figura 3.2, vemos que se pueden crear 6 códigos distintos. ♢

Una herramienta fundamental para resolver tal tipo de problemas es el siguiente enunciado cuya validez puede comprobarse facilmente utilizando un diagrama de árbol.

Principio Fundamental del Conteo *Si una tarea A puede realizarse de n formas y otra tarea B puede hacerse de m formas, entonces la tarea que consiste en realizar primero A y luego B puede hacerse de $n.m$ formas distintas.*

Observar que este principio puede extenderse a una mayor cantidad de tareas, como vemos en el siguiente ejemplo.

Ejemplo 109. ¿De cuántas formas puede vestirse una persona que tiene 3 pares de zapatos, 4 pantalones, 2 camisas y 5 sacos? Como tiene 3 posibilidades para elegir zapatos y 4 posibilidades para elegir pantalones, resulta que tiene $3.4 = 12$ formas de

vestir pantalones y zapatos. Además, como tiene 2 posibilidades para elegir camisas, resulta que tiene 12.2 = 24 formas de vestir zapatos, pantalón y camisa. Finalmente, como tiene 5 posibilidades para elegir saco, obtenemos que puede vestirse de 24.5 = 120 formas distintas.

Observar que el resultado obtenido es 3.4.2.5= 120 pues deviene de la secuencia de tareas: ponerse zapatos-pantalón-camisa-saco. $\diamondsuit$

En lo que sigue utilizaremos el principio fundamental para la deducción de varias fórmulas que son de utilidad para resolver problemas de conteo.

Se llama **número de variaciones de n elementos tomados de a k**, se denota $V_{n,k}$, a la cantidad de formas en que se puede hacer una lista ordenada de longitud k utilizando elementos de un conjunto con cardinal n, y prohibiendo que en la lista aparezcan elementos repetidos.

Ejemplo 110. Para calcular el número de variaciones de 4 tomados de a 2, debemos ver cuantas listas ordenadas de longitud 2 podemos hacer con 4 elementos, no permitiendo elementos repetidos. Llamemos a, b, c y d a estos elementos. Que la lista sea ordenada significa que no es lo mismo a-b que b-a. Para hacer una lista de longitud 2 debemos realizar 2 tareas: elegir el primer elemento y luego elegir el segundo. El primer elemento se puede elegir de 4 formas distintas y el segundo de 3 formas distintas pues, como no se puede repetir, habrá un elemento que no puede ser elegido en segundo lugar. Tenemos que $V_{4,2} = 4.3 = 12$. Efectivamente, es fácil ver que las posibles listas son:

$$\begin{array}{ccc} a-b & a-c & a-d \\ b-a & b-c & b-d \\ c-a & c-b & c-d \\ d-a & d-b & d-c \end{array}$$

$\diamondsuit$

Teorema 111. *Para todo par de números naturales n y k, con $k \leq n$, vale que*

$$V_{n,k} = \frac{n!}{(n-k)!}$$

.

Demostración: Como vimos en el ejemplo anterior, se trata de elegir el primer elemento de la lista entre los n elementos dados, luego el segundo entre los $n-1$

que restan, luego el tercero entre los $n-2$ que quedan, y así sucesivamente hasta elegir el elemento k-ésimo de la lista entre los $n-(k-1)$ que quedan luego de haber elegido los $k-1$ primeros elementos de la lista. Entonces, por el princio fundamental enunciado precedentemente, la lista se puede hacer de

$$n.(n-1).(n-2)...(n-(k-1)) = \frac{n!}{(n-k)!}$$

formas . □

El número de variaciones es útil para tratar problemas del estilo de los que a continuación se proponen como ejercicios (al final del capítulo se desarrollan varios ejemplos):

Se quiere elegir 3 alumnos entre los 30 que concurren a clase para ocupar respectivamente los cargos de Presidente, Secretario y Tesorero de una comisión. ¿De cuántas formas distintas se puede hacer? ¿De cuántas si 2 personas determinadas no pueden ser presidente? ¿De cuántas si una de cuatro personas determinadas debe ser Tesorero?

¿Cuántos números de 5 cifras distintas pueden formarse? ¿Cuántos menores que 50.000?

De una caja conteniendo 10 bolillas numeradas se extrae al azar una bolilla, luego se repite este procedimiento otras cuatro veces. ¿cuál es la probabilidad de haber sacado la secuencia de números 1-2-3-4-5? ¿Y la de haber sacado la secuencia 2-4-6-8-10?

Se llama **número de permutaciones de n elementos**, se denota P_n, a la cantidad de formas en que se pueden ordenar n elementos. Es claro que ordenar n elementos dados es lo mismo que formar con ellos una lista de longitud n sin repeticiones, entonces, por el teorema anterior, tenemos el siguiente resultado.

Teorema 112. *Para todo $n \in \mathbb{N}$ vale que $P_n = n!$.*

Demostración: Es claro que $P_n = V_{n,n} = \frac{n!}{(n-n)!} = n!$. □

El número de variaciones es útil para tratar problemas del estilo de los que a continuación se proponen como ejercicios (al final del capítulo se desarrollan varios ejemplos):

¿Cuántos anagramas de la palabra MONEDA se pueden formar?

¿De cuántas formas pueden ordenarse 7 personas en una fila. ¿De cuántas si dos de ellas no pueden estar juntas?

¿De cuántas formas distintas pueden sentarse 10 personas alrededor de una mesa redonda?

¿De cuántas formas pueden ordenarse 5 libros H, G, M, L, y F en una bibiblioteca? ¿De cuántas si G y H deben estar juntos? ¿De cuántas si L y M no deben estar juntos?

Se llama **número de variaciones con repetición de n elementos tomados de a k**, se denota $V^*_{n,k}$, a la cantidad de formas en que se puede hacer una lista ordenada de longitud k utilizando elementos de un conjunto con cardinal n, y permitiendo que en la lista aparezcan elementos repetidos.

Ejemplo 113. Para calcular el número de variaciones con repetición de 4 tomados de a 2, debemos ver cuantas listas ordenadas de longitud 2 podemos hacer con 4 elementos. Llamemos a, b, c y d a estos elementos. Para hacer una lista de longitud 2 debemos realizar 2 tareas: elegir el primer elemento y luego elegir el segundo. El primer elemento se puede elegir de 4 formas distintas y el segundo también de 4 formas distintas pues las repeticiones están permitidas. Tenemos que $V^*_{4,2} = 4.4 = 4^2 = 16$ Efectivamente, las listas son:

$$\begin{array}{cccc} a-a & a-b & a-c & a-d \\ b-a & b-b & b-c & b-d \\ c-a & c-b & c-c & c-d \\ d-a & d-b & d-c & d-d \end{array}$$



Teorema 114. *Para todo par de números natuales n y k, vale que $V^*_{n,k} = n^k$.*

Demostración: Como vimos anteriormente, se trata de elegir el primer elemento de la lista entre los n elementos dados, luego elegir el segundo también entre los n dados, y así sucesivamente hasta elegir el elemento k-ésimo de la lista, siempre entre los n elementos dados, pues no está prohibido repetir. Entonces, por el princio fundamental enunciado precedentemente, la lista se puede hacer de n^k formas distintas. □

El número de variaciones con repetición es útil para tratar problemas del estilo de los que a continuación se proponen como ejercicios (al final del capítulo se desarrollan varios ejemplos):

De una caja conteniendo 10 bolillas numeradas se extrae al azar una bolilla, se anota el número obtenido y se devuelve la bolilla a la caja; luego se repite este procedimiento otras cuatro veces. ¿cuál es la probabilidad de haber sacado la secuencia de números 1-2-3-4-5? ¿ Y la de haber sacado 1-1-1-1-1?

Cantidad de números de 6 cifras que se pueden formar con las cifras 2,4,6,8. ¿Y con las cifras 0,1,2,...,9?

Cantidad de Patentes que se han emitido al finalizar las que empiezan con la letra F.

Se llama **número de combinaciones de n elementos tomados de a k**, se denota $C_{n,k}$, a la cantidad de subconjuntos con cardinal k que tiene un conjunto con cardinal n.

Ejemplo 115. Para determinar el número de combinaciones de 4 elementos tomados de a dos, debemos determinar la cantidad de subconjuntos con 2 elementos tiene un conjunto con 4 elementos. Llamemos a, b, c y d a esos elementos. A diferencia de lo que hicimos en los casos anteriores, no podemos utilizar el principio fundamental. Como los elementos de un subconjunto no están ordenado (es lo mismo $\{a, b\}$ que $\{b, a\}$), no se trata de elegir primero un elemento y luego otro, sino que elegimos los dos a la vez.
Lo que podemos hacer en este caso es pensar que cada subconjunto con 2 elemento da origen a $P_2 = 2!$ listas ordenadas, entonces

$$C_{4,2}.P_2 = C_{4,2}.2! = V_{4,2} = \frac{4!}{(4-2)!},$$

de donde $C_{4,2} = \frac{4!}{(4-2)!2!} = 6$. Efectivamente, los subconjuntos con 2 elementos de $\{a, b, c, d\}$ son

$$\begin{array}{ccc} \{a,b\} & \{a,c\} & \{a,d\} \\ \{b,c\} & \{b,d\} & \{c,d\}. \end{array}$$

♢

Teorema 116. *Para todo par de números naturales n y k, con $k \leq n$, vale que*

$$C_{n,k} = \frac{n!}{(n-k)!k!} = \binom{n}{k}.$$

Demostración: Como vimos en el ejemplo anterior, cada subconjunto de tamaño k da origen a $P_k = k!$ listas sin repetición de longitud k. Luego, la cantidad de variaciones sin repetición de n tomados de a k es $C_{n,k}.k!$, de donde resulta que

$$C_{n,k} = \frac{V_{n,k}}{k!} = \frac{n!}{(n-k)!k!}.$$

□

El número de combinaciones es útil para tratar problemas del estilo de los que a continuación se proponen como ejercicios (al final del capítulo se desarrollan varios ejemplos):

¿De cuántas formas puedo formar una comisión con 3 integrantes elegidos entre los 30 alumnos de una clase? ¿De cuántas si dos personas determinadas no pueden estar juntas en la comisión?

¿De cuántas formas puedo formar un grupo de 4 personas si se las elige entre 4 hombres y 7 mujeres dados? ¿Cuántos si al menos debe haber 1 hombre en el grupo? ¿Cuántos si debe haber 2 hombres y 2 mujeres?

En una caja conteniendo 10 bolillas numerdas se introduce la mano y se sacan 5 bolillas. ¿Cuál es la probabilidad de haber obtenido los números 1,2,3,4 y 5?

Se tienen 11 bolillas numeradas, 6 blancas y 5 negras. Se toman 4 al azar, ¿cuántos resultados posibles hay? ¿Cuántos si se toman 2 blancas y dos negras? ¿Cuántos si se deben tomar las 4 de igual color?

Finalmente veremos un problema que involucra elementos indistinguibles. Comenzaremos por dar un par de ejemplos para que se entienda el concepto.

Ejemplo 117.

- ¿Cuántos anagramas de la palabra ANA se pueden formar?

  Si la palabra tuviese todas sus letras distintas la respuesta sería claramente $P_3 = 3! = 6$, pero como la letra A está repetida y la primer A es indistinguible de la segunda, debo pensar de otra manera.

  Este caso es muy sencillo y puedo ver cuales son las soluciones:

  ANA AAN NAA (I)

  Las usaremos para inferir una idea general aplicable a cualquier otro caso similar.

  Supongamos que considero la misma palabra pero distinguiendo las A, es decir considero la palabra ANA’. Sabemos que la cantidad de formas en que se pueden ordenar estas letras es 3!=6, a saber:

  ANA’ AA’N NAA’

  A’NA A’AN NA’A (II)

Observar, comparando (I) y (II), que cada una de las soluciones del problema considerado está contada aquí dos veces pues las dos letras repetidas se pueden ordenar de $P_2 = 2! = 2$ formas distintas. Es decir, si llamamos x a la cantidad de anagramas de ANA, tenemos que

$$x.2! = \text{ cantidad de anagramas de ANA'} = 3!$$

resulta que $x = \frac{3!}{2!} = 3$ como habíamos visto precedentemente.

- ¿Cuántos anagramas de la palabra ANANA se pueden formar?

  Repitamos la idea del ejemplo anterior, distinguiendo momentaneamente las letras: ANA'N'A"; estas se pueden permutar de $P_5 = 5! = 1200$ formas distintas. Cada solución del problema planteado, es decir, cada anagrama de ANANA, está contado aquí 3!.2! pues la letra A está repetida 3 veces (A, A' y A" se pueden ordenar de 3! formas distintas) y la letra N está repetida 2 veces (N y N' se pueden ordenar de 2! formas distintas), resulta que si llamamos x a la cantidad cantidad de anagramas de ANANA tenemos que

$$x.3!.2! = \text{ cantidad de anagramas de ANA'N'A"} = 5!$$

  de donde $x = \frac{5!}{3!.2!} = 10$.

  Efectivamente los anagramas de ANANA son

  AAANN NNAAA NAAAN

  AANNA ANNAA

  AANAN NANAA ANAAN NAANA ANANA



Estamos en condiciones de enunciar el siguiente teorema.

Teorema 118. *Dados n elementos de k clases distintas, en cantidades n_i para $1 \leq i \leq k$ (n_1 de la clase 1, n_2 de la clase 2,...,n_k de la clase k); si los elementos de una misma clase son indistinguibles entonces la cantidad de formas en que pueden ordenarse los n elementos es*

$$\frac{n!}{n_1!\ n_2!\ ...\ n_k!}.$$

La formulación anterior es útil para resolver problemas del estilo de los que a continuación se proponen como ejercicios (al final del capítulo se desarrollan varios ejemplos):

Cantidad de anagramas de palabras con letras repetidas.

Cantidad de maneras en que se pueden extrar 5 bolillas de una urna en la que hay 3 bolillas rojas, 6 blancas, 3 azules y 2 rojas.

Ordenar libros en un estante cuando hay 8 de Historia iguales entre sí, 5 de Matemática iguales entre sí y 3 de Geografía iguales entre sí.

3.3.1. Ejemplos varios

1) ¿Cuántos números de 5 cifras distintas pueden formarse utilizando los dígitos 1,2,3,5,7,8,9?

Rta: cada número corresponde a una lista ordenada de longitud 5 y sin repeticiones, por lo tanto, la cantidad es $V_{7,5} = \frac{7!}{(7-5)!} = \frac{7!}{2!}$.

¿Cuántos de ellos son números pares?

Rta: para que el número sea par debe terminar en 2 o en 8. Para formar los que terminan en 2 basta elegir las primeras 4 cifras entre 1,3,5,7,8,9, por lo tanto, son $V_{6,4} = \frac{6!}{2!}$. Lo mismo para los que terminan en 8; luego, la cantidad de numeros pares que pueden formarse es $2.\frac{6!}{2!}$.

¿Cuántos de ellos son mayores que 50000?

Rta: para que un número de 5 cifras ($\neq 0$) sea mayor que 50000, basta que la primer cifra sea mayor o igual que 5, en el caso de este ejercicio la primer cifra podrá ser 5, 7, 8, o 9; resulta, pensando como en el caso anterior, que la cantidad de números mayores que 50000 es $4.\frac{6!}{2!}$.

¿En cuántos de ellos los dígitos 8 y 9 aparecen juntos?

Hay dos casos: cuando aparece la secuencia 89 y cuando aparece 98.

En el primer caso podemos pensar así: como ya sabemos que tenemos que usar 89, nos falta elegir las 3 cifras restantes entre los dígitos 1,2,3,5,7; esto podemos hacerlo de $C_{5,3}$ formas distintas. Ahora, cada uno de los grupos formados tiene 4 elementos: los 3 dígitos elegidos y 89 que no puede separarse, por lo tanto puede ordenarse de 4! formas distintas. Lo mismo ocurre con los números en que aparece la secuencia 98. Resulta que la cantidad que queremos calcular es $2.C_{5,3}.4!$

2) ¿Cuántos números de 5 cifras no necesariamente distintas entre sí pueden formarse

utilizando los dígitos 1,2,3,5,7,8,9?

Rta: cada número corresponde a una lista ordenada de longitud 5 y se permiten repeticiones, por lo tanto la cantidad es $V^*_{7,5} = 7^5$.

¿Cuántos de ellos son números pares?

Rta: para que el número sea par debe terminar en 2 o en 8. Para formar los que terminan en 2 basta elegir las primeras 4 cifras entre 1,2,3,5,7,8,9 pues se puede repetir, por lo tanto son $V^*_{7,4} = 7^4$. Lo mismo para los que terminan en 8, por lo tanto la cantidad de numeros pares es 2.7^4.

¿Cuántos de ellos son capicúa (se leen igual de izquierda a derecha que de derecha a izquierda?

Rta:Si queremos formar números capicúa nos basta elegir las 3 primeras (o últimas) cifras, pues las restantes estarán obligadas a ser iguales a éstas, resulta que la cantidad de capicúas es $V^*_{7,3} = 7^3$.

3) En el directorio de una sociedad hay 10 hombres y 6 mujeres. Se quiere formar una comisión revisora formada por 5 de estas personas, ¿de cuántas formas distintas puede quedar constituída la comisión?

Rta: se trata de elegir un grupo (subconjunto) de 5 personas entre las 16 que forman el directorio, por lo tanto se puede hacer de $C_{16,5} = \frac{16!}{11!5!}$ formas distintas.

¿De cuantas si Juan y Marcela no pueden estar juntos en la comisión?

Rta: al total de posibilidades debemos restarle aquellas en las que Juan y Marcela están juntos, que son $C_{14,3}$, pues se trata de elegir a los restantes 3 integrantes de la comisión entre los restantes 14 miembros del directorio. Resulta que la cantidad de comisiones posibles en las que Juan y Marcela no estén juntos es $C_{16,5} - C_{14,3}$.

¿De cuántas si debe haber al menos 3 mujeres?

Rta: podemos contar aquellas con exactamente 3 mujer, aquellas con exactamente 4 y aquellas con exactamente 5 mujeres, y sumarlas.

Para contar las que tienen exactamente 3 mujeres: pensamos en elegir las tres mujeres entre las 6 que hay en el directorio, esto puede hacerse de $C_{6,3}$; luego en elegir a 2 hombres para completar la comisión, esto puede hacerse de $C_{(10,2)}$; por el principio fundamenta resulta que en total hay $C_{6,3}.C_{10,2}$ comisiones posibles con exactamente 3 mujeres.

Análogamente, hay $C_{6,4}.C_{10,1}$ comisiones posibles con exactamente 4 mujeres; y hay

$C_{6,5}.C_{10,0}$ comisiones posibles con exactamente 5 mujeres.

Resulta que la cantidad de comisiones con al menos 3 mujeres es

$$C_{6,3}.C_{10,2} + C_{6,4}.C_{10,1} + C_{6,5}.C_{10,0}.$$

4) Se tiene 4 cajas numeradas (caja 1, caja 2, caja 3, caja 4) y 50 bolillas indistinguibles entre sí. Se quiere repartir las bolillas en las cajas, ¿de cuántas formas puede hacerse?

Rta: para ayudar a comprender la pregunta, el siguiente cuadro muestra algunas soluciones posibles.

caja 1	caja 2	caja 3	caja 4
50	0	0	0
0	50	0	0
0	0	50	0
0	0	0	50
49	1	0	0
49	0	1	0
49	0	0	1
...	...	...	...

Asumamos que un símbolos * representan una bolilla y que / representa la división entre una caja y otra; así tenemos que, por ejemplo:

**/* // significa 2 bolillas en caja 1, 1 bolilla en caja 2, 0 bolilla en caja 3 y 0 en caja 4;

/**//* significa 0 bolilla en caja 1, 2 bolillas en caja 2, 0 bolilla en caja 3 y 1 bolilla en caja 4;

///*** significa 0 bolilla en caja 1, 0 bolilla en caja 2, 0 bolilla en caja 3 y 3 bolilla en caja 4.

Usando esta simbolización, el problema de distribuir 50 bolillas indistinguibles en 4 cajas distinguibles equivale a hallar todas las permutaciones posibles de 50 simbolos * y 3 simbolos /; como sabemos, esto puede hacerse de $\frac{53!}{50!3!}$ formas distintas.

¿De cuantas formas puede hacerse si en la primer caja debe haber al menos 5 bolillas y en la última caja debe haber al menos 10 bolillas?

Rta: comienzo por poner 5 bolillas en la caja 1, 10 bolillas en la caja 4 y reparto de cualquier forma las restantes $50 - 5 - 10 = 35$ bolillas; por lo tanto se puede hacer de $\frac{38!}{35!3!}$ formas distintas.

6) Si las variables representan números naturales, ¿cuántas soluciones tiene la ecuación $x + y + z = 10$?

Rta: podemos pensar que cada variable es una caja y que estamos repartiendo 10 bolilas (unidades) en ellas; así tenemos, como en el ejemplo anterior, que las soluciones posibles son $\frac{12!}{10!2!} = 66$.

Capítulo 4

Números enteros y números racionales

4.1. Números enteros

Un número real se dice **entero** si es cero o es un número natural o es el opuesto de un número natural. Si indicamos con $-\mathbb{N}$ al subconjunto de $\mathbb{R}$ formado por los opuestos de los números naturales, es decir, $-\mathbb{N} = \{x : -x \in \mathbb{N}\} = \{-1, -2, -3, \cdots\}$, resulta que el conjunto de los números enteros, denotado $\mathbb{Z}$, es

$$\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}.$$

En el capítulo anterior vimos que tanto la suma como el producto de números reales son operaciones cerradas en el conjunto de los naturales. Veremos ahora que lo mismo ocurre en el conjunto de los enteros.

Proposición 119. *Las operaciones + y . definidas en $\mathbb{R}$ son cerradas en $\mathbb{Z}$: la suma de dos números enteros es un número entero y el producto de dos número enteros es también un número entero. Además, si $x \in \mathbb{Z}$ entonces $-x \in \mathbb{Z}$.*

Demostración: Primero probemos que el opuesto de un entero es un entero. Si $x = 0$ entonces $-x = 0 \in \mathbb{Z}$; si $x \in \mathbb{N}$ entonces $-x \in -\mathbb{N} \subset \mathbb{Z}$; y si $x \in -\mathbb{N}$ entonces $-x \in \mathbb{N} \subset \mathbb{Z}$.

Sean a y b números enteros; para probar que la suma y el producto son cerrados en $\mathbb{Z}$, basta consider los siguientes casos:

$a = 0$: entonces $a + b = 0 + b = b \in \mathbb{Z}$ y $a.b = 0.b = 0 \in \mathbb{Z}$.

$a \in \mathbb{N}$ y $b \in \mathbb{N}$: entonces, por lo probado en el capítulo anterior, $a + b \in \mathbb{N}$ y $a.b \in \mathbb{N}$; como $\mathbb{N} \subset \mathbb{Z}$, resulta que $a + b \in \mathbb{Z}$ y $a.b \in \mathbb{Z}$.

$a \in -\mathbb{N}$ y $b \in -\mathbb{N}$: entonces $-a \in \mathbb{N}$ y $-b \in \mathbb{N}$, de donde $(-a) + (-b) = -(a + b) \in \mathbb{N} \subset \mathbb{Z}$, resulta $a + b \in \mathbb{Z}$. Por otra parte, $a.b = (-a).(-b) \in \mathbb{N} \subset \mathbb{Z}$.

$a \in \mathbb{N}$ y $b \in -\mathbb{N}$: entonces $a \in \mathbb{N}$ y $-b \in \mathbb{N}$. Si $a = -b$, la demostración es trivial. Si $a > -b$ entonces, por la Proposición 94, $a - (-b) = a + b \in \mathbb{N} \subset \mathbb{Z}$. Análogamente, si $a < -b$ entonces $-b - a = -(a + b) \in \mathbb{N}$, de donde $a + b \in \mathbb{Z}$. Finalmente, $a.(-b) = -(a.b) \in \mathbb{N} \subset \mathbb{Z}$, luego $a.b \in \mathbb{Z}$. □

Potencias con exponente entero de un número real: extendemos la definición de potencia con exponente natural de la siguiente forma, $a^{-m} = (a^{-1})^m$ para cualquier $m \in \mathbb{N}$.

Ejercicio 120.

Probar que $a^{-m} = (a^m)^{-1}$ para todo $m \in \mathbb{N}$. Probar que las propiedades enunciadas en el Ejercicio 103 del capítulo anterior para exponentes naturales, también valen para el caso de exponentes enteros. ♢

Se dice que un número entero b no nulo **divide** a un número entero a, si existe $k \in \mathbb{Z}$ tal que $a = k.b$. En tal caso también se dice que b es **divisor** de a, o que a es **divisible** por b, o que a es **múltiplo** de b. En general, b divide a a se denota $\mathbf{b} \mid \mathbf{a}$; y b no divide a a se indica $\mathbf{b} \nmid \mathbf{a}$.

Ejemplo 121.

- 1 es divisor de m para todo $m \in \mathbb{Z}$ pues $m = m.1$.
- Todo número entero no nulo m es divisor de sí mismo pues $m = 1.m$.
- Todo número entero no nulo m es divisor de 0 pues $0 = 0.m$.
- $b \mid a \;\leftrightarrow\; -b \mid a \;\leftrightarrow\; -b \mid -a \;\leftrightarrow\; b \mid -a$ pues
  $a = k.b = (-k).(-b)$ si y sólo si $-a = -(k.b) = (-k).b = k.(-b)$. ♢

Proposición 122. *Si a y b son enteros no nulos y $b \mid a$ entonces $\mid b \mid \leq \mid a \mid$.*

Demostración: Como $b \mid a$ entonces existe $k \in \mathbb{Z}$ tal que $a = k.b$. Resulta que $\mid a \mid = \mid k.b \mid = \mid k \mid . \mid b \mid \geq 1. \mid b \mid = \mid b \mid$, donde usamos que $\mid k \mid \geq 1$, lo cual se satisface pues $k \in \mathbb{Z}$ y $k \neq 0$. □

Ejercicio 123.

Sean a, b y c enteros. Probar que

1. $a \mid 1 \leftrightarrow \mid a \mid = 1$.
2. $(a \mid b \wedge b \mid a) \leftrightarrow \mid a \mid = \mid b \mid$.
3. $(a \mid b \wedge b \mid c) \to a \mid c$.
4. $(a \mid b \wedge a \mid c) \to (a \mid b + c \wedge a \mid b - c)$. ♢

Un número entero se dice **primo**, si tiene exactamente cuatro divisores. Es claro que si p es primo entonces $-p$ es primo.

Ejemplo 124.

- 0 no es primo, ya vimos que tiene una cantidad infinita de divisores.
- 1 no es primo, ya vimos que tiene exactamente dos divisores que son 1 y -1.
- 2 es primo. Efectivamente, si d divide a 2, entonces $\mid d \mid \leq \mid 2 \mid = 2$. Como d es un entero debe ser $\mid d \mid = 2$ o $\mid d \mid = 1$ de donde los únicos divisores de 2 son: 2, -2, 1 y -1. ♢

Puede decirse también que p es primo si y sólo si $p \neq \pm 1$ y los únicos divisores de p son 1, -1, p y $-p$.

La llamada **Criba de Erastóstenes** nos permite visualizar los primero números primos positivos. Consideremos una tabla en la que aparecen los primeros números naturales.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Iremos remarcando los números primos y tachando los que no lo son. Observar que:

> (*) un número natural n mayor que 1 es primo si y sólo si $d \nmid n$ para todo natural d con $1 < d < n$.

Comenzamos tachando el 1 porque no es primo. Luego sigue 2 que es primo, lo remarcamos. Todo número de la forma $2.k$ con $k \geq 2$ no es primo por (*)(2 lo divide y $1 < 2 < 2.k$), lo tachamos.

~~1~~	$\boxed{2}$	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

El primer número no remarcado ni tachado es 3, él es primo por (*), lo remarcamos. Nuevamente, Todo número de la forma $3.k$ con $k \geq 2$ no es primo por (*)(3 lo divide y $1 < 3 < 3.k$), lo tachamos.

~~1~~	$\boxed{2}$	$\boxed{3}$	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

El primer número no remarcado ni tachado es 5, él es primo por (*), lo remarcamos. Nuevamente, Todo número de la forma $5.k$ con $k \geq 2$ no es primo por (*)(5 lo divide y $1 < 5 < 5.k$), lo tachamos.

~~1~~	$\boxed{2}$	$\boxed{3}$	~~4~~	$\boxed{5}$	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Continuando con este procedimiento obtenemos la siguiente tabla en la que aparecen remarcados los números primos.

~~1~~	$\boxed{2}$	$\boxed{3}$	~~4~~	$\boxed{5}$	~~6~~	$\boxed{7}$	~~8~~	~~9~~	~~10~~
$\boxed{11}$	~~12~~	$\boxed{13}$	~~14~~	~~15~~	~~16~~	$\boxed{17}$	~~18~~	$\boxed{19}$	~~20~~
~~21~~	~~22~~	$\boxed{23}$	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	$\boxed{29}$	~~30~~
$\boxed{31}$	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	$\boxed{37}$	~~38~~	~~39~~	~~40~~
$\boxed{41}$	~~42~~	$\boxed{43}$	~~44~~	~~45~~	~~46~~	$\boxed{47}$	~~48~~	~~49~~	~~50~~
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Ejercicio 125.

Verificar que los números primos menores o iguales que 200 son:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199. $\diamondsuit$

Proposición 126. *Todo número entero distinto de 1 o -1 es divisible por algún número primo.*

Demostración: Sea a un número entero distintos de 1 y de -1. Si $a = 0$, la proposición es verdadera pues, por ejemplo, 2 es primo y 2 divide a 0.

Si $a \geq 2$, probaremos por inducción sobre a (principio fuerte) que a es divisible por algún número primo.

Para $a = 2$, la proposición es verdadera pues 2 es primo y 2 divide a 2.

Sea $k \geq 2$ cualquiera y asumamos que la proposición es verdadera para cada entero positivo s con $2 \leq s \leq k$; es decir: para cada entero positivo s con $2 \leq s \leq k$, se verifica que existe algún primo que divide a s. Veremos que la proposición se cumple para $a = k + 1$.

Si $k + 1$ es primo, la proposición vale pues $k + 1$ divide a $k + 1$.

Si $k+1$ no es primo entonces existe un entero positivo d, $d \neq \pm 1$ y $d \neq \pm(k+1)$, tal que d divide a $k+1$; además, como d divide a $k+1$ debe ser $d \leq k+1$. Así $2 \leq d \leq k$, entonces, por hipótesis inductiva, existe un primo p que divide a d; el mismo primo p divide a $k + 1$, como queríamos probar.

Finalmente, si $a \leq -2$ entonces $-a \geq 2$. Por lo demostrado anteriormente existe un primo que divide a $-a$; el mismo primo divide a a. $\square$

Supongamos que quiero saber si un número entero positivo dado, digamos 101, es primo. Para ello basta saber si existe un primo p menor que 101 tal que p divide a

101. Ocurre que los primos menores que 101 son varios: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 y 97.
Para simplificar esta tarea podemos usar la siguiente proposición.

Proposición 127. *Sea $n \in \mathbb{N}$, $n \neq 1$. Si para todo primo p tal que $p^2 \leq n$ se verifica que p no divide a n, entonces n es primo.*

Demostración: Como $n \neq 1$, por la Proposición 126, existe algún primo que divide a n, luego el conjunto $A = \{p \in \mathbb{N} : p \text{ primo y } p \text{ divide a } n\}$ es un subconjunto no vacío de $\mathbb{N}$. Como $\mathbb{N}$ es un conjunto bien ordenado, A tiene primer elemento, sea p_0. Como p_0 divide a n, existe $k \in \mathbb{N}$ tal que $n = k.p_0$. Si $k \neq 1$, entonces, por la Proposición 126, existe p_1 primo positivo, tal que p_1 divide a k, luego p_1 divide a n. Por la elección de p_0, es $p_0 \leq p_1$; como además $p_1 \leq k$, tenemos que $p_0 \leq k$. Luego $(p_0)^2 = p_0.p_0 \leq k.p_0 = n$. Esto contradice la hipótesis que cualquier primo cuyo cuadrado es menor o igual que n no divide a n, la contradicción proviene de suponer $k \neq 1$.
Resulta $k = 1$ de donde $n = 1.p_0 = p_0$ es primo, como queríamos probar. □

Ejemplo 128.
Para saber si 101 es primo basta ver si 2, 3, 5 o 7 dividen a 101 pues estos son los únicos primos cuyos respectivos cuadrados son menores o iguales que 101. Observar que $11^2 = 121 > 101$. Es fácil ver que ninguno de estos números divide a 101, por lo tanto 101 es primo. ♢

Proposición 129. *El conjunto de los número primos es infinito.*

Demostración: Supongamos que el conjunto $\mathcal{P}$ de los números primos es finito, entonces existe $n \in \mathbb{N}$ tal que $\mathcal{P} = \{p_1, p_2, p_3, \cdots, p_n\}$. Sea $m = p_1.p_2.p_3.\cdots.p_n + 1$; es claro que $m \neq 1$, entonces, por la Proposición 126, existe un primo que divide a m. Sin pérdida de generalidad podemos suponer que este primo que divide a m es p_1. Luego existe $k \in \mathbb{Z}$ tal que $m = k.p_1$; esto es $p_1.p_2.p_3.\cdots.p_n + 1 = k.p_1$, de donde $1 = k.p_1 - p_1.p_2.p_3.\cdots.p_n = p_1.(k - p_2.p_3.\cdots.p_n)$. Resulta que p_1 divide a 1, lo cual contradice que p_1 es primo. La contradicción proviene de suponer que $\mathcal{P}$ es finito, concluimos que $\mathcal{P}$ es infinito. □

Teorema 130 (Algoritmo de la división en $\mathbb{Z}$)**.** *Dados números enteros a y d, $d \neq 0$, existe un único par de números enteros q y r tales que:*

$$a = q.d + r \quad y \quad 0 \leq r <\mid d \mid .$$

Se dice que q es el ***cociente*** *de la división de a por d; y que r es el* ***resto*** *de la división de a por d.*

Demostración: Primero probaremos la existencia de q y r, luego la unicidad.
Si d divide a a entonces existe $k \in \mathbb{Z}$ tal que $a = k.d$. De donde obtenemos que la proposición es verdadera considerando $q = k$ y $r = 0$.
Asumamos que d no divide a a. Esto implica $a \neq 0$ y $d \neq 1$. Sea $A = \{x \in \mathbb{N} :$ existe un entero k tal que $x = a - k.d\}$. Observar que si $a > 0$ entonces $a - 0.d \in A$, y si $a < 0$ entonces $a - (a.d).d = a.(1 - d^2) \in A$. Luego, en cualquier caso, A es un subconjunto no vacío de $\mathbb{N}$. Como $\mathbb{N}$ está bien ordenado, A tiene primer elemento, sea r. Resulta que $r > 0$ y existe $q \in \mathbb{Z}$ tal que $r = a - q.d$; así, $a = q.d + r$. Para probar que q y r satisfacen las condiciones pedidas en el enunciado del teorema, resta ver que $r <\mid d \mid$.
Observar que $r \neq\mid d \mid$, pues, en otro caso, d dividiría a a.
Supongamos que $r >\mid d \mid$, entonces $h = r- \mid d \mid\in \mathbb{N}$ y $h = (a - q.d)- \mid d \mid= a - (q \pm 1).d$; luego, $h \in A$. Como r es el primer elemento de A, debe ser $r \leq h = r- \mid d \mid$, de donde $\mid d \mid\leq 0$. Resulta $d = 0$, lo cual contradice las hipótesis del teorema. Como la contradicción proviene de suponer $r >\mid d \mid$ y sabemos que $r \neq\mid d \mid$, obtenemos que $r <\mid d \mid$.
Veamos ahora que q y r son los únicos enteros que satisfacen lo pedido. Efectivamente, supongamos que q' y r' satisfacen que

$$a = q'.d + r' \quad \text{y} \quad 0 \leq r' <\mid d \mid .$$

Si $r' = 0$ entonces $q.d + r = q'.d$. Obtenemos que $\mid r \mid=\mid (q' - q) \mid . \mid d \mid<\mid d \mid$. Resulta que $q = q'$ y luego $r = r' = 0$.
Si $r' \neq 0$ entonces $r' \in A$, luego $r \leq r'$ y así tenemos que $r' - r =\mid r' - r \mid<\mid d \mid$. Además, $0 = a - a = (q'.d + r') - (q.d + r) = (q' - q).d + (r' - r)$, de donde $\mid q' - q \mid . \mid d \mid=\mid r' - r \mid<\mid d \mid$. Se deduce que $q = q'$ y luego $r = r' = 0$. □

Ejemplo 131.

- Como $130 = 8.15 + 10$ y $0 \leq 10 < 15$ tenemos que el resto de dividir 130 por

15 es 10, y el cociente es 8.

Observar que aunque $130 = 8.15 + 10$ no podemos decir que 10 es el resto de dividir a 130 por 8 puesto que $10 \not< 8$; en efecto, $130 = 8.15+10 = 8.15+8+2 = 8.16 + 2$, luego el resto de dividir a 130 por 8 es 2. Ahora sí, como $2 < 16$, podemos decir que el resto de dividir a 130 por 16 es 2.

- Para determinar resto y cociente en casos en que el **dividendo** a o el **divisor** d sean negativos, primero se considera $\mid a \mid$ y $\mid d \mid$ y luego se procede como en los siguientes ejemplos sumando y restando el divisor si es necesario.
- Hallar cociente y resto de dividir a -50 por 13.

  Sabemos que $50 = 3.13+11$, luego $-50 = (-3).13-11 = (-3).13-13+13-11 = (-4).13 + 2$; resulta que el cociente pedido es -4 y el resto es 2.
- Hallar cociente y resto de dividir 50 por -13.

  Como antes, $50 = 3.13+11$, luego $50 = (-3).(-13)+11$. Resulta que el cociente pedido es -3 y el resto 11.
- Hallar cociente y resto de dividir -50 por -13.

  Otra vez, $50 = 3.13 + 11$ luego $-50 = 3.(-13) - 11 = 3.(-13) - 13 + 13 - 11 = 4.(-13) + 2$. Resulta que el cociente pedido es 4 y el resto 2. ♢

Proposición 132. *[Propiedades del resto]. Indicaremos mediante $r_d(a)$ al resto de la división de a por d.*

1. $d \mid a \leftrightarrow r_d(a) = 0$.
2. $r_d(a + b) = r_d(r_d(a) + r_d(b))$.
3. $r_d(a \cdot b) = r_d(r_d(a) \cdot r_d(b))$.
4. $r_d(a^n) = r_d([r_d(a)]^n)$.

Demostración: La demostración de 1. es trivial. Demostraremos 2. y dejaremos 3. y 4. como ejercicios.

Sean q y q' los cocientes de dividir a a y a b por d, respectivamente; luego

$$a = q.d + r_d(a) \quad \text{y} \quad 0 \leq r_d(a) <\mid d \mid .$$

$$b = q'.d + r_d(b) \quad \text{y} \quad 0 \leq r_d(b) <\mid d \mid .$$

Sumando estas expresiones tenemos que $a+b=(q+q').d+(r_d(a)+r_d(b))$.

No puedo decir que $r_d(a)+r_d(b)$ sea el resto de dividir $a+b$ por d porque no sé si $r_d(a)+r_d(b)<|d|$. Luego dividimos $r_d(a)+r_d(b)$ por d. Por el algoritmo de la división tenemos que

$$r_d(a)+r_d(b)=q''.d+r_d(r_d(a)+r_d(b)) \quad \text{y} \quad 0\leq r_d(r_d(a)+r_d(b))<|d|\,.$$

Reemplazando en la expresión anterior obtenemos
$a+b=(q+q').d+(r_d(a)+r_d(b))=(q+q').d+(q''.d+r_d(r_d(a)+r_d(b)))=(q+q'+q'').d+r_d(r_d(a)+r_d(b))$ y como $0\leq r_d(r_d(a)+r_d(b))<|d|$, resulta que $r_d(a+b)=r_d(r_d(a)+r_d(b))$, como queríamos probar. □

Ejemplo 133.

Determinar el resto de dividir 2^{93} por 3 y el resto de dividir 9^{45} por 7.

$r_3(2^{93})=r_3(2.2^{92})=r_3(r_3(2).r_3(4^{46}))=r_3(2.[r_3(4)]^{46})=r_3(2.1^{46})=r_3(2)=2.$

$r_7(9^{45})=r_7([r_7(9)]^{45})=r_7(2^{45})=r_7(8^{15})=r_7([r_7(8)]^{15})=r_7(1^{15})=r_7(1)=1.$ ♢

Ejercicio 134.

1. Sea $n\in\mathbb{Z}$. Probar que n es par si y solo si n^2 es par.
2. Sea $n\in\mathbb{Z}$. Determinar los posibles restos de la división de n^2 por 3.
3. Probar que la suma de los cuadrados de 3 números enteros no divisibles por 3, es un múltiplo de 3. ♢

Sean a y b enteros cualesquiera. Se dice x que es una **combinación lineal entera** de a y b, si existen enteros s y t tales que $x=s.a+t.b$; es claro que, en tal caso, $x\in\mathbb{Z}$. Por ejemplo, 2 es combinación entera de 462 y de 180 pues $2=3.462+(-7).180$. ¿1 es combinación entera de 462 y 180?

Ejercicio 135.

Probar que si h es un **divisor común** de a y de b, esto es, h divide a a y h divide a b, entonces h divide a toda combinación lineal entera de a y b. ♢

En lo que sigue, relacionaremos el máximo común divisor de dos enteros con sus combinaciones enteras. Probaremos que x es combinación entera de a y b si y sólo si x es un múltiplo del máximo común divisor de a y b.

Teorema 136 (Existencia y unicidad del máximo común divisor)**.** *Sean a y b enteros, no ambos nulos. Existe un único $d\in\mathbb{N}$, tal que:*

i) $d \mid a$ *y* $d \mid b$*; y*

ii) para todo entero h *se verifica que si* $h \mid a$ *y* $h \mid b$ *entonces* $h \mid d$.

Observar que, como consecuencia de *ii*), cualquier divisor común de a y de b es menor o igual que d, por eso d se llama **máximo común divisor** de a y b, se denota (a, b).

Demostración: Sea $A = \{x \in \mathbb{N} : x \text{ es una combinación entera de } a \text{ y } b\}$. Observar que $a^2 + b^2 \in A$, luego A es un subconjunto no vacío de $\mathbb{N}$. Como $\mathbb{N}$ es un conjunto bien ordenado, A tiene primer elemento, sea d; es claro que $d \in \mathbb{N}$ y existen enteros s y t tales que $d = s.a + t.b$. Veremos que d satisface lo pedido en el enunciado del teorema.

Por el algoritmo de la división, existen enteros q y r tales que $a = q.d + r$ con $0 \leq r < d$; luego $r = a - q.d = a - q(s.a + t.b) = (1 - q.s).a + (-q.t).b$ es una combinación entera de a y b. Como $r \notin A$, pues $r < d$ y d es primer elemento de A, debe ser que $r \notin \mathbb{N}$, resulta $r \leq 0$, y entonces $r = 0$. Obtenemos que $a = q.d$, es decir $d \mid a$. Análogamente se prueba que $d \mid b$.

Finalmente, la condición *ii*) se cumple pues d es combinación entera de a y b (Ver ejercicio anterior).

Ahora supongamos existe otro entero positivo d' que satisface *i*) y *ii*).

Como tenemos que

$$(d \mid a \wedge d \mid b) \text{ y } (h \mid a \wedge h \mid b \rightarrow h \mid d'); \text{ resulta que } d \mid d'.$$

Análogamente, como vale que

$$(d' \mid a \wedge d' \mid b) \text{ y } (h \mid a \wedge h \mid b \rightarrow h \mid d); \text{ obtenemos que } d' \mid d;$$

Así, $d \mid d'$ y $d' \mid d$, luego $d = d'$ pues ambos son positivos. Esto prueba la unicidad del máximo común divisor. □

Corolario 137. *El máximo común divisor* (a, b) *es la menor combinación lineal entera positiva de* a *y* b*. En particular, si 1 es combinación entera de* a *y* b *entonces* $(a, b) = 1$*, pues no habrá otra combinación entera positiva menor. Además,* x *es una combinación entera de* a *y* b *si y sólo si* x *es un múltiplo de* (a, b).

Ejemplo 138.

Sean a y b enteros no nulos. Por la propia definición de máximo común divisor, es trivial que

$(a, b) = (a, -b) = (-a, -b) = (-a, b)$.

$(a, 1) = 1 \quad (a, a+1) = 1 \quad (a, a) =\mid a \mid$.

$a \mid b \leftrightarrow (a, b) =\mid a \mid$.

Si p es primo y p no divide a a entonces $(a, p) = 1$.

$\diamondsuit$

El siguiente resultado es la base del **algoritmo de Euclides** que permite el cálculo de (a, b) mediante una secuencia de divisiones.

Proposición 139. *Si a y b son enteros positivos entonces $(a, b) = (b, r_b(a))$.*

Demostración: Por simplicidad escribamos $r = r_b(a)$ y $d = (b, r_b(a))$. Veremos que d satisface las condiciones del Teorema 136, luego podremos concluir que $d = (a, b)$.
$d \mid a$ pues $a = q.b + r_b(a)$ y d divide a b y a $r_b(a)$.
$d \mid b$ pues $d = (b, r_b(a))$.
Sea h cualquiera tal que $h \mid a$ y $h \mid b$. Como $r_b(a) = a - q.b$ resulta que $h \mid r_b(a)$; tenemos entoces que $h \mid b$ y $h \mid r_b(a)$ de donde $h \mid (b, r_b(a)) = d$. $\square$

Ejemplo 140. Como haciendo las divisiones tenemos que

$$462=2\ .180 + 82 \qquad 180=2\ .82 + 16$$
$$82=5\ .16 + 2 \qquad 16= 8\ .2 + 0$$

resulta

$$(462, 180) = (180, 82) = (82, 16) = (16, 2) = (2, 0) = 2.$$

$\diamondsuit$

Proposición 141. *Si p es primo y $p \mid a.b$ entonces $p \mid a$ o $p \mid b$.*

Demostración: Sea p un primo que divide a $a.b$ (existe $k \in \mathbb{Z}$ tal que $a.b = k.p$) y supongamos que p no divide a a. Luego, $(a, p) = 1$, de donde se deduce que existen enteros s y t tales que $1 = s.a + t.p$. Multiplicando por b obtenemos $b = s.a.b + t.p.b = s.k.p + t.p.b = p.(s.k + t.b)$; como $s.k + t.b \in \mathbb{Z}$ resuta que p divide a b. $\square$

Ejercicio 142.

1. Probar por inducción en n que si p es primo y p divide al producto $a_1.a_2.\cdots.a_n$ entonces existe un i, $1 \leq i \leq n$, tal que p divide a a_i.

2. Probar que si a y b son enteros no nulos entonces, para todo natural n, se satisface que $(a^n, b^n) = (a, b)^n$. $\diamondsuit$

Dos número enteros a y b se dicen **coprimos** si $(a, b) = 1$.

Ejemplo 143.

Son coprimos:

- a y $a + 1$, para a un entero cualquiera. Efectivamente, $1 = (-1).a + 1.(a + 1)$, luego $(a, a + 1) = 1$.
- p y q, para p y q primos distintos cualesquiera. Efectivamente, como (p, q) divide a p debe ser $(p, q) = 1$ o $(p, q) = p$; y como (p, q) divide a q debe ser $(p, q) = 1$ o $(p, q) = q$. Dado que $p \neq q$ obtenemos que $(p, q) = 1$.
- p y $(p - 1)!$, para p primo cualquiera mayor que 2. Efectivamente, como $d = (p, (p - 1)!)$ divide a p debe ser $d = 1$ o $d = p$. Supongamos que $d = p$, entonces p divide a $(p - 1)! = (p - 1).(p - 2). \cdots . 2.1$.

  Por lo probado en el ejercicio anterior, debe existir i con $1 \leq i \leq p - 1$ tal que p divide a $p - i$, lo cual es una contradicción pues $0 \leq p - i < p$. La contradicción proviene de suponer que $d = p$, luego $d \neq p$. Resulta $d = 1$.
- $\frac{a}{(a,b)}$ y $\frac{b}{(a,b)}$, para a y b enteros cualesquiera no nulos.

  Observar que, como (a, b) divide a a, existe $k \in \mathbb{Z}$ tal que $a = k.(a, b)$. Luego, $\frac{a}{(a,b)} = k \in \mathbb{Z}$. Análogamente, $\frac{b}{(a,b)} \in \mathbb{Z}$.

  Sean s y t enteros tales que $(a, b) = s.a + t.b$. Resulta que $1 = s.\frac{a}{(a,b)} + t.\frac{b}{(a,b)}$, luego $(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$. $\diamondsuit$

Ejercicio 144. Sean a y b coprimos y $n \in N$. Probar que:

1. Si $a \mid n$ y $b \mid n$ entonces $a.b \mid n$.
2. Si $a \mid b.n$ entonces $a \mid n$.
3. Mostrar ejemplos que prueven que 1. y 2. no son ciertas si a y b no son coprimos.
4. Probar que si p es un primo positivo entonces p divide a $\begin{pmatrix} p \\ i \end{pmatrix}$ para todo i tal que $1 \leq i \leq p - 1$. $\diamondsuit$

Una **ecuación lineal diofántica** en las incógnitas x e y es una ecuación lineal con coeficientes enteros que requiere soluciones enteras, es decir, una ecuación del tipo

$a.x+b.y=c$ donde a, b y c son enteros y x e y toman valores enteros. Como vimos en el Corolario 137, esta ecuación tiene solución sí y solo sí (a,b) divide a c, o en otras palabras, si c es un múltiplo de (a,b). El siguiente enunciado ofrece también la forma de las soluciones de una ecuación diofántica.

Proposición 145. *Sean a, b y c enteros. La ecuación $a.x+b.y=c$ tiene solución en el conjunto de los número enteros sí y solo sí $(a,b) \mid c$.*
Más aún, cuando $(a,b) \mid c$, la ecuación tiene una cantidad infinita de soluciones: si s y t son enteros tales que $(a,b)=s.a+t.b$, entonces, para cada $m \in \mathbb{Z}$, tenemos una solución x_m, y_m de la ecuación dada haciendo

$$\begin{cases} x_m = s.\frac{c}{(a,b)} - m.\frac{b}{(a,b)} \\ y_m = t.\frac{c}{(a,b)} + m.\frac{a}{(a,b)} \end{cases}$$

Demostración: Es fácil ver que, para cualquier $m \in Z$, $a.(s.\frac{c}{(a,b)} - m.\frac{b}{(a,b)}) + b.(t.\frac{c}{(a,b)} + m.\frac{a}{(a,b)}) = c$. Luego, x_m, y_m es solución de la ecuación dada.
Veamos que toda solución entera tiene esta forma para algún $m \in \mathbb{Z}$: sea x e y una solución cualquiera de la ecuación dada, como $x_0 = s.\frac{c}{(a,b)}$, $y_0 = t.\frac{c}{(a,b)}$ es solución, tenemos que

$$\begin{array}{rcl} a.(s.\frac{c}{(a,b)}) + b.(t.\frac{c}{(a,b)}) & = & c \\ a.x+b.y & = & c \\ \hline a.(s.\frac{c}{(a,b)} - x) + b.(t.\frac{c}{(a,b)} - y) & = & 0. \end{array}$$

Resulta $a.(s.\frac{c}{(a,b)} - x) = b.(y - t.\frac{c}{(a,b)})$, de donde $\frac{a}{(a,b)}.(s.\frac{c}{(a,b)} - x) = \frac{b}{(a,b)}.(y - t.\frac{c}{(a,b)})$. Como $\frac{a}{(a,b)}$ y $\frac{b}{(a,b)}$ son coprimos tenemos que $\frac{a}{(a,b)}$ divide a $y - t.\frac{c}{(a,b)}$, luego existe $m \in \mathbb{Z}$ tal que $y - t.\frac{c}{(a,b)} = m.\frac{a}{(a,b)}$, es decir, $y = t.\frac{c}{(a,b)} + m.\frac{a}{(a,b)}$. Ahora, reeemplazando esta expresión de y en la formulación anterior tenemos $a.(s.\frac{c}{(a,b)} - x) = m.\frac{a}{(a,b)}$, de donde $x = s.\frac{c}{(a,b)} - m.\frac{b}{(a,b)}$, como queríamos probar. □

Ejemplo 146.

- La ecuación $15.x+20.y=8$ no tiene soluciones enteras pues $(15,20)=5$ no divide a 8.
- La ecuación $15.x+20.y=10$ tiene infinitas soluciones enteras; como $(15,20) = 5 = 1.20+(-1).15$, las soluciones enteras de esta ecuación son

$$x_m = (-1).\frac{10}{5} - m.\frac{20}{5} = -2 - m.4 \qquad y_m = 1.\frac{10}{5} + m.\frac{15}{5} = 2 + m.3.$$

Por ejemplo, $x_0 = -2$ e $y_0 = 2$ es solución, se obtiene haciendo $m = 0$.

$x_1 = -6$ e $y_1 = 5$ es solución, se obtiene haciendo $m = 1$. ♢

Teorema 147 (Existencia y unicidad del mínimo común múltiplo). *Sean a y b enteros no nulos. Existe un único número $m \in \mathbb{N}$, tal que:*

i) $a \mid m$ *y* $b \mid m$; *y*

ii) para todo entero h se verifica que si $a \mid h$ y $b \mid h$ entonces $m \mid h$.

Observar que, como consecuencia de ii), cualquier múltiplo común de a y de b es mayor o igual que m, por eso m se llama **mínimo común múltiplo** de a y b; se denota $[\mathbf{a}, \mathbf{b}]$.

Demostración: Sea $A = \{x \in \mathbb{N} : a \mid x \wedge b \mid x\}$. Observar que A es un subconjunto no vacío de $\mathbb{N}$, por ejemplo $\mid a.b \mid \in A$. Como $\mathbb{N}$ es un conjunto bien ordenado, A tiene primer elemento, sea m. Es fácil verificar que m satisface la condición i). Para ver que satisface ii), consideremos h divisible por a y por b. Por el algoritmo de la división, existen enteros q y r tales que $h = q.m + r$ y $0 \leq r < m$; luego, r es divisible por a y por b. Como $r \notin A$ porque $r < m$ y m es el primer elemento de A, debe ser $r = 0$, de donde concluimos que $m \mid h$. La unicidad se prueba suponiendo existe $m' \in \mathbb{N}$ que también satisface las condiciones anteriores y luego , en forma análoga a la utilizada en el Teorema 137, se obtiene que $m = m'$. □

Ejemplo 148. Sean a y b enteros positivos. Por la propia definición de mínimo común múltiplo es trivial que

- $[a, b] = [a, -b] = [-a, -b] = [-a, b]$.
- $[a, 1] = [a, a] = a$.
- $[a, b] = a \leftrightarrow b \mid a$. ♢

Proposición 149. *Si a y b son enteros no nulos entonces $\mid a.b \mid = (a, b).[a, b]$*

Demostración: Sin pérdida de generalidad podemos suponer que a y b son positivos. Sea $m = \frac{a.b}{(a,b)} = \frac{a}{(a,b)}.b = a.\frac{b}{(a,b)}$; veremos que $m = [a, b]$, con lo cual habremos probado que $a.b = (a, b).[a, b]$.

Es claro que $m \in \mathbb{N}$ y que a y b dividen a m. Sea $h \in \mathbb{Z}$ tal que $a \mid h$ y $b \mid h$, veremos que $m \mid h$. Efectivamente, existen enteros s y t tales que $(a, b) = s.a + t.b$, luego $1 = s.\frac{a}{(a,b)} + t.\frac{b}{(a,b)}$; multiplicando por h resulta $h = s.\frac{a}{(a,b)}.h + t.\frac{b}{(a,b)}.h$. Como

existen enteros k y k' tales que $h = a.k = b.k'$, reemplazando en la expresión anterior obtenemos $h = s.\frac{a}{(a,b)}.k'.b + t.\frac{b}{(a,b)}.k.a = \frac{a.b}{(a,b)}(s.k' + t.k) = m.(s.k' + t.k)$; como $s.k' + t.k \in \mathbb{Z}$ hemos probado que $m \mid h$. □

Los conceptos de máximo común divisor y mínimo común múltiplo que hemos visto se pueden extender a una mayor cantidad de elementos, es decir, si $a_1, a_2, \cdots, a_n$ son enteros no nulos, existe un único número $d \in \mathbb{N}$, tal que:

i) $d \mid a_1,\ d \mid a_2, \cdots\ d \mid a_n$; y

ii) para todo entero h, si $h \mid a_1,\ h \mid a_2, \cdots\ \ h \mid a_n$ entonces $h \mid d$.

El entero positivo d se llama **máximo común divisor** de $a_1, a_2, ...$ y a_n, en general se denota $(a_1, a_2, ..., a_n)$ y se satisface que $(a_1, a_2, ..., a_n) = ((a_1, a_2, ..., a_{n-1}), a_n))$.

Análogamente, existe un único número $m \in \mathbb{N}$, tal que:

i) $a_1 \mid m,\ a_2 \mid m, \ \cdots\ a_n \mid m$; y

ii) para todo entero h, si $a_1 \mid h,\ a_2 \mid h, \cdots\ a_n \mid h$ entonces $m \mid h$.

m se llama **mínimo común múltiplo** de $a_1, a_2, ...$ y a_n, en general se denota $[a_1, a_2, ..., a_n]$ y se satisface que $[a_1, a_2, ..., a_n] = [[a_1, a_2, ..., a_{n-1}], a_n]]$.

Ejemplo 150.

$(10, 15, 35) = ((10, 15), 35) = (5, 35) = 5.$

$[10, 15, 35] = [[10, 15], 35] = [30, 35] = 210.$

♢

Teorema 151 (Teorema Fundamental de la Aritmética). *Sea m un número entero distinto de 0, 1 y -1. Existen número primos positivos $p_1 \leq p_2 \leq ... \leq p_k$ tales que*

$$m = \xi.p_1.p_2....p_k$$

*donde $\xi = 1$ o $\xi = -1$. Esta escritura (que se llama **descomposición de** m **en factores primos** o **factorización de** m **en primos**) es única, es decir, si p'_1, p'_2, $\cdots$ p'_s son primos positivos tales que: $p'_1 \leq p'_2 \leq ... \leq p'_s$ y*

$$m = \delta.p'_1.p'_2....p'_s, \text{ donde } \delta = 1 \text{ o } \delta = -1$$

entonces $k = s$, $\xi = \delta$, y $p_i = p'_i$ para todo $i = 1, ..., k$.

Demostración: Observar que basta probar que todo entero mayor que 1 se factoriza en primos.
Sea $S = \{n \in \mathbb{Z} : n > 1 \text{ y } n \text{ no se factoriza en primos}\}$. Como todo primo positivo p se factoriza en primos haciendo $p = 1.p$, resulta que

$$S \text{ no contiene números primos.} \tag{4.1}$$

Supongamos $S \neq \emptyset$. En tal caso, como $S \subset \mathbb{N}$ y $\mathbb{N}$ es un conjunto bien ordenado, S tiene primer elemento, sea n_0.
Como $n_0 \in S$, sabemos que n_0 es distinto de 1 y de -1; luego, por Teorema 126, existe algún primo positivo que divide a n_0. Sea p_0 el menor primo positivo que divide a n_0; y sea $m \in \mathbb{N}$ tal que $n_0 = m.p_0$.
Observar que $m < n_0$, luego $m \notin S$. Pero $m > 1$ (pues si $m = 1$ resulta que $n_0 = p_0$ contradiciendo (4.1)), entonces debe ser que m se factoriza en primos, es decir, existen primos positivos $p_1 \leq p_2 \leq ... \leq p_k$ tales que $m = p_1.p_2....p_k$.
Como p_0 es el menor primo positivo que divide a n_0 tenemos $p_0 \leq p_1 \leq p_2 \leq ... \leq p_k$ y $n_0 = p_0.m = p_0.p_1.p_2....p_k$, luego n_0 se factoriza, lo cual contradice que $n_0 \in S$.
La contradicción proviene de suponer $S \neq \emptyset$, entonces concluimos que $S = \emptyset$ y así todo entero mayor que 1 se factoriza en primos.
Unicidad: supongamos que m se factoriza en primos de dos formas distintas, es decir:

$$m = p_1.p_2...p_k = p'_1.p'_2...p'_h$$

con primos positivos $p_1 \leq p_2 \leq ... \leq p_k$ y $p'_1 \leq p'_2 \leq ... \leq p'_h$.

Observar que como p_1 es primo y p_1 divide a $p'_1.p'_2...p'_h$, entonces existe i tal que $p_1 = p'_i$. Análogamente, existe j tal que $p'_1 = p_j$.
Ahora, $p_1 = p'_i \geq p'_1 = p_j \geq p_1$, con lo cual son todos iguales, es decir $p_1 = p'_1$.
Simplificando resulta $p_2...p_k = p'_2...p'_h$; repitiendo el razonamiento anterior obtenemos $p_2 = p'_2$ y así sucesivamente. Resulta que k debe ser igual a h y $p_1 = p'_1$, $p_2 = p'_2$,...,$p_k = p'_k$. $\square$
Dado $m \in \mathbb{Z}$, $m \neq 0$, para cada primo positivo p llamamos

$$v_p(m) = mayor\{i \in \mathbb{N}_0 \ / \ p^i \mid m\};$$

en otras palabras $v_p(m)$ es la cantidad de veces que el primo p aparece en la factorización de m.

Ejemplo 152. m =2.2.2.3.11.13.13= $2^3.3^1.11^1.13^2$, luego $v_2(m) = 3$; $v_3(m) = 1$; $v_{11}(m) = 1$; $v_{13}(m) = 2$; y $v_p(m) = 0$ para cualquier otro primo positivo p. ♢

Corolario 153. *Sean a y b enteros no nulos. Se satisface que:*

1. $v_p(a.b) = v_p(a) + v_p(b)$ *para todo primo positivo p.*
2. *b divide a a* $\leftrightarrow v_p(b) \leq v_p(a)$ *para todo primo positivo p.*
3. *Si b divide a a, entonces* $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$ *para todo primo positivo p.*
4. *Si $k \in \mathbb{N}$, entonces* $v_p(a^k) = k.v_p(a)$ *para todo primo positivo p.*
5. $v_p((a,b)) = menor\{v_p(a), v_p(b)\}$ *para todo primo positivo p.*
6. $v_p([a,b]) = mayor\{v_p(a), v_p(b)\}$ *para todo primo positivo p.*

Demostración: es consecuencia directa de la unicidad del Teorema Fundamental de la Aritmética. □

Ejemplo 154.

- $a = 3^2.7^3.11 \quad b = 2.3.5^4.13$
  $a.b = 2.3^3.5^4.7^3.11.13$
  $(a,b) = 3^1$ y $[a,b] = 2.3^2.5^4.7^3.11.13$
- Se dice que un entero m es un **cuadrado perfecto** si existe $n \in \mathbb{Z}$ tal que $m = n^2$. Observar que m es un cuadrado perfecto si y sólo si $v_p(n)$ es par para todo primo positivo p. Por ejemplo, 6552 no es un cuadrado perfecto pues su factorización en primos es 2.2.2.3.3.7.13= $2^3.3^2.7.13$.
  Si queremos hallar el menor número natural n tal que $6552.n$ sea un cuadrado perfecto, podemos proceder de la siguiente manera:
  Como para todo primo positivo p,
  $$v_p(6552.n) = v_p(6552) + v_p(n),$$
  por lo dicho antes, para que $6552.n$ sea un cuadrado perfecto, necesitamos que $v_p(n)$ sea par si $v_p(6552)$ es impar y viceversa. Como además queremos n lo más chico posible, debemos tomar $v_2(n) = 1$, $v_7(n) = 1$, $v_{13}(n) = 1$ y $v_p(n) = 0$, para cualquier otro primo p; luego, $n = 2.7.13 = 182$ es el menor entero positivo tal que multiplicado por 6525 resulta un cuadrado perfecto. Efectivamente $6552.182 = 2^4.3^2.7^2.13^2$=$(2^2.3.7.13)^2 = 1092^2$.

Observar que en forma análoga podemos ver que no existe un entero positivo impar n tal que 6552.n sea un cuadrado perfecto.

Si queremos determinar el menor entero positivo m tal que 6552.m sea un cubo perfecto tendremos que elegir $v_3(m) = 1$, $v_7(m) = 2$ y $v_{13}(m) = 2$; por lo tanto la solución es $m = 3.7^2.13^2 = 24843$. Efectivamente, $6552.24843 = (2.3.7.13)^3$

Ahora, si quiero determinar el mayor cuadrado perfecto que divide a 6552, se trata de $2^2.3^2 = 36$

- Veamos que no existen enteros no nulos n y m tales que $n^2 = 180.m^4$. Si así fuera, es decir, si $n^2 = 180.m^4$ entonces, para todo primo positivo p, debería cumplirse que $v_p(n^2) = v_p(180.m^4)$, de donde $2.v_p(n) = v_p(180) + v_p(m^4)$, entonces $2.v_p(n) = v_p(2^2.3^2.5) + 4.v_p(m)$. En particular para $p = 5$, debe ser $2.v_5(n) = v_5(2^2.3^2.5) + 4.v_5(m)$; pero entonces, como $v_5(2^2.3^2.5) = 1$, resulta $2.v_5(n) = 1 + 4.v_5(m)$, luego $2.(v_5(n) - 2.v_5(m)) = 1$, lo cual contradice el hecho que los únicos divisores enteros de 1 son 1 y -1. Resulta que tales n y m no existen. ♢

Proposición 155. *Sean p_1, p_2, $\cdots$ p_k primos positivos distintos entre sí y n_1, n_2, $\cdots$ n_k números naturales. La cantidad de divisores positivos de $m = p_1^{n_1}.\ p_2^{n_2}. \cdots .p_n^{n_k}$ es igual a $(n_1 + 1).(n_2 + 1). \cdots .(n_k + 1)$.*

Demostración: para que un entero positivo d sea divisor de m, por el punto 2. del Corolario 153, debe cumplirse que $0 \leq v_p(d) \leq v_p(m)$ para cada primo p; luego tenemos que $0 \leq v_{p_1}(d) \leq v_{p_1}(m) = n_1$, $0 \leq v_{p_2}(d) \leq v_{p_2}(m) = n_2$, $\cdots$ $0 \leq v_{p_k}(d) \leq v_{p_k}(m) = n_k$ y $v_p(d) = 0$ para cualquier otro primo p. Resulta que en la factorización de d, el exponente de cada primo p_i puede tomar $n_i + 1$ valores distintos, luego d puede tomar $(n_1 + 1).(n_2 + 1). \cdots .(n_k + 1)$ valores distintos, como queríamos probar. □

Ejemplo 156. Como $20 = 2^2.5$ la cantidad de divisores positivos de 20 es 3.2=6. Efectivamente, ellos son: $2^0.5^0$=1; $2^0.5^1$=5; $2^1.5^0$=2; $2^1.5^1$=10; $2^2.5^0$=4 y $2^2.5^1$=20.

Si quiero determinar un múltiplo de 20 que tenga exactamente 10 divisores positivos, puedo pensar de la siguiente manera. Llamemos m al número que estoy buscando. Para que m sea múltiplo de 20 debe ser $v_2(m) \geq 2$ y $v_5(m) \geq 1$; luego podemos escribir $m = 2^{v_2(m)}.5^{v_5(m)}.p_1^{v_{p_1}(m)}.p_2^{v_{p_2}(m)}...$ donde los p_i son primos distintos de 2 y 5.

Resulta que la cantidad de divisores positivos de m es

$$(v_2(m)+1).(v_5(m)+1).(v_{p_1}(m)+1).(v_{p_1}(m)+1)... = 10 = 2.5.$$

Luego, como $v_2(m) \geq 2$ y $v_5(m) \geq 1$, debe ser $v_2(m)+1 = 5$; $v_5(m)+1 = 2$ y $v_{p_i}(m)+1 = 1$ para cualquier otro primo p_i.
Así tenemos que $v_2(m) = 4$ y $v_5(m) = 1$; entonces $m = 2^4.5 = 80$. Efectivamente, 80 es múltiplo de 20 y tiene exactamente 10 divisores positivos: 1, 2, 4, 8, 16, 5, 10, 20, 40 y 80. ♢

4.1.1. Congruencias

Sea n un número natural. Se dice que un entero a es **congruente** módulo n con un entero b si n divide a $a-b$, es decir, si $n \mid a-b$. Para indicar que a es congruente con b módulo n escribiremos $a \equiv b \ mod(n)$. Por ejemplo 15 es congruente con 7 módulo 4 pues $15-7 = 8 = 2.4$; luego escribimos $15 \equiv 7mod(4)$.
La relación **congruencia módulo** n es una relación de equivalencia en $\mathbb{Z}$. Efectivamente, es reflexiva pues para todo entero a se verifica que $n \mid a-a = 0$; es simétrica, pues $n \mid a-b$ si y sólo si $n \mid b-a$; y es transitiva porque si $n \mid a-b$ y $n \mid b-c$ entonces $n \mid (a-b)+(b-c) = a-c$. El conjunto cociente de $\mathbb{Z}$ por $\equiv \ mod(n)$ se indica $\mathbb{Z}_n$ (Ver Sección 2.0.6 del Capítulo 2).
Como la relación es simétrica, podemos decir a es congruente con b o b es congruente con a o a y b son congruentes.
La siguiente proposición ofrece una manera alternativa de definir la relación congruencia módulo n.

Proposición 157. *$a \equiv b \ mod(n)$ si y sólo si $r_n(a) = r_n(b)$.*

Demostración: Por el algoritmo de la división $a = q.n + r_n(a)$ y $b = q'.n + r_n(b)$ con $0 \leq r_n(a) < n$ y $0 \leq r_n(b) < n$. Podemos suponer, sin pérdida de generalidad, $r_n(a) \geq r_n(b)$ y así tenemos que $0 \leq r_n(a) - r_n(b) < n$. Restando las expresiones anteriores obtenemos $a-b = (q-q')n + r_n(a) - r_n(b)$. Como $0 \leq r_n(a) - r_n(b) < n$ entonces

$$r_n(a) - r_n(b) = r_n(a-b).$$

Resulta $r_n(a) - r_n(b) = 0$ si y sólo si $r_n(a-b) = 0$, como queríamos probar. □

Corolario 158. *Para todo $n \in \mathbb{N}$, el conjunto cociente $\mathbb{Z}_n$ tiene exactamente n elementos.*

Ejemplo 159.
$\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ donde
$\overline{0} = \{x \in \mathbb{Z} : r_3(x) = r_3(0)\} = \{x \in \mathbb{Z} : x = 3.k \text{ con } k \in \mathbb{Z}\} = 3.\mathbb{Z};$
$\overline{1} = \{x \in \mathbb{Z} : r_3(x) = r_3(1)\} = \{x \in \mathbb{Z} : x = 3.k + 1 \text{ con } k \in \mathbb{Z}\} = 3.\mathbb{Z} + 1;$ y
$\overline{2} = \{x \in \mathbb{Z} : r_3(x) = r_3(2)\} = \{x \in \mathbb{Z} : x = 3.k + 2 \text{ con } k \in \mathbb{Z}\} = 3.\mathbb{Z} + 2.$ $\diamondsuit$

Convención: dados a y b enteros cualesquiera, $a.\mathbb{Z} + b$ indica el subconjunto de $\mathbb{Z}$ formado por todos aquellos enteros x tales que existe $k \in \mathbb{Z}$ satisfaciendo que $x = a.k + b$.

La siguiente propiedad puede expresarse en forma sintética diciendo que la relación de congruencia es **compatible** con la suma y el producto de enteros.

Proposición 160. *Si $a \equiv c\ mod(n)$ y $b \equiv d\ mod(n)$, entonces*

$a + b \equiv c + d\ mod(n),$
$a - b \equiv c - d\ mod(n),$
$a.b \equiv c.d\ mod(n),$ *y*
$a^k \equiv c^k\ mod(n)$ *para todo natural k.*

Demostración: Usaremos la Proposición 132: $r_n(a + b) = r_n(r_n(a) + r_n(b)) = r_n(r_n(c)+r_n(d)) = r_n(c+d))$. Análogamente se pueban las otras relaciones; la última, por inducción sobre k. $\square$

Ejercicio 161. Probar que si para todo i entre 1 y m, $a_i \equiv b_i mod(n)$, entonces

$$(\sum_{i=1}^{m} a_i) \equiv (\sum_{i=1}^{m} b_i)\, mod(n) \quad \text{y} \quad (\prod_{i=1}^{m} a_i) \equiv (\prod_{i=1}^{m} b_i)\, mod(n).$$



Ejemplo 162.

- usaremos los resultados anteriores para demostrar el **criterio de divisibilidad** por 3: Un número es divisible por 3 si y solo sí la suma de sus dígitos lo es.
  Por ejemplo,
  2345 no es divisible por 3 pues 2 + 3 + 4 + 5 = 14 no es múltiplo de 3.
  445566 es divisible por 3 pues 4 + 4 + 5 + 5 + 6 + 6 = 30 es múltiplo de 3.

Nos basaremos en el **desarrollo decimal** del número: cualquier entero positivo m se puede escribir como la suma de una cantidad finita de términos en la forma

$$\sum_{i\geq 0} a_i.(10)^i$$

donde cada a_i es un entero tal que $0 \leq a_i \leq 9$. La existencia y unicidad de este desarrollo es una consecuencia directa del algoritmo de la división. Los coeficientes a_i son los **dígitos** de m.

Para los números de los ejemplos anteriores el desarrollo decimal es:

$2345 = 2.10^3 + 3.10^2 + 4.10^1 + 5.10^0$.

$445566 = 4.10^5 + 4.10^4 + 5.10^3 + 5.10^2 + 6.10^1 + 6.10^0$.

En lo que sigue, por simplicidad, solo escribiremos $\equiv$ en lugar de $\equiv mod(3)$.

Como $10 \equiv 1$, entonces, por la Proposición 160, $10^i \equiv 1^i$, de donde $10^i \equiv 1$ para todo $i \geq 1$. Ahora, como $10^i \equiv 1$ y $a_i \equiv a_i$, entonces $a_i.10^i \equiv a_i.1$; luego, $a_i.10^i \equiv a_i \quad$ para todo $i \geq 1$.

Resulta, usando lo probado en el ejercicio anterior, que $\sum_i a_i.10^i \equiv \sum_i a_i$, es decir, $m \equiv \sum_i a_i$, como queríamos probar.

En rigor hemos demostrado que, dado un número entero positivo m, el resto de dividir a m por 3 es igual al resto de dividir a la suma de sus dígitos por 3.

Siguiendo con el ejemplo anterior, tenemos que

$$r_3(2345) = r_3(2+3+4+5) = r_3(14) = r_3(1+4) = r_3(5) = 2.$$

- Calcular el resto de dividir a $34^{7865} - 6^{3578}$ por 35. En lo que sigue $\equiv$ significa $\equiv mod(35)$. Como $34-(-1) = 35$, entonces $34 \equiv -1$, de donde $34^{7865} \equiv (-1)^{7865} \equiv -1$. Además, como $36 \equiv 1$, entonces $6^{3578} \equiv (6^2)^{1789} \equiv 36^{1789} \equiv 1^{1789} \equiv 1$. Resulta que $34^{7865} - 6^{3578} \equiv -1 - 1 \equiv -2$. Como $33 - (-2) = 35$, entonces $33 \equiv -2$. Así tenemos que $34^{7865} - 6^{3578} \equiv 33$ de donde concluimos que el resto de dividir a $34^{7865} - 6^{3578}$ por 35 es igual a 33.
- En forma similar a la utilizada para probar el criterio de divisibilidad por 3, se puede probar que si $m = \sum_i a_i.10^i$ es el desarrollo decimal del entero positivo m, entonces el resto de dividir m por 11 es igual al resto de dividir a $\sum_i(-1)^i.a_i$ por 11.

  Por ejemplo, $r_{11}(11) = r_{11}(1-1) = r_{11}(0) = 0$;

$r_{11}(111) = r_{11}(1-1+1) = r_{11}(1) = 1$, luego 111 no es múltiplo de 11;

$r_{11}(1111) = r_{11}(1-1+1-1) = r_{11}(0) = 0$;

$r_{11}(9754) = r_{11}(9-7+5-4) = r_{11}(3) = 3$

Hallar un múltiplo de 11 capicúa con 8 dígitos, los cuatro primeros distintos entre sí:

puede ser 12344321 pues $1-2+3-4+4-3+2-1 = 0$. Efectivamente, $11.112221 = 12344321$.

Observar que todo número capicúa con una cantidad par de cifras es múltiplo de 11. ¿Qué puede decir de los capicúas con una cantidad impar de cifras? $\diamondsuit$

Teorema 163 (Euler-Fermat-Vivaldi)**.** *Sea p primo positivo. Para todo natural n vale que $n^p \equiv n \ mod(p)$.*

Demostración: En lo que sigue $\equiv$ significa $\equiv mod(p)$. Haremos inducción sobre n: la proposición es verdadera si $n = 1$, pues $1^p = 1$. Sea $k > 1$ y asumamos que $k^p \equiv k \ mod(p)$, veremos que la proposición se satisface para $k+1$. Por comodidad escribiremos sólo $\equiv$.

Recordando que si p es primo entonces p divide al número combinatorio $\begin{pmatrix} p \\ i \end{pmatrix}$ para todo i tal que $0 < i < p$, tenemos que existe $h \in \mathbb{Z}$ tal que

$$(k+1)^p = \sum_{0 \le i \le p} \begin{pmatrix} p \\ i \end{pmatrix} k^i = \begin{pmatrix} p \\ 0 \end{pmatrix} + h.p + \begin{pmatrix} p \\ p \end{pmatrix} k^p.$$

Entonces $(k+1)^p = 1 + h.p + k^p$, esto es $(k+1)^p \equiv 1 + k^p$.

Como por hipótesis inductiva $k^p \equiv k \ mod(p)$, resulta que $(k+1)^p \equiv 1 + k^p \equiv 1 + k$, como queríamos probar. $\square$

Ejemplo 164. dado un primo cualquiera, por ejemplo 7, y un entero cualquiera por ejemplo 88, vale que 7 divide a $88^7 - 88$. Efectivamente, $88^7 - 88 = 40867559636992 - 88 = 40867559636904 = 7.5838222805272$. $\diamondsuit$

Corolario 165. *Sea p primo positivo. Si $(n,p) = 1$ entonces $n^{p-1} \equiv 1 \ mod(p)$.*

Demostración: como $1 = r.n + s.p$ entonces $1 \equiv r.n \equiv r.n^p = r.n.n^{p-1} \equiv 1.n^{p-1} = n^{p-1}$, donde $\equiv$ indica $\equiv mod(p)$. $\square$

4.2. Números racionales

Un número real x se dice **racional** si existen enteros a y b, $b \neq 0$, tales que $x = \frac{a}{b} = a.b^{-1}$. El subconjunto de $\mathbb{R}$ formado por los números racionales se indica con $\mathbb{Q}$.

Proposición 166. *Las operaciones + y . definidas en $\mathbb{R}$ son cerradas en $\mathbb{Q}$*

Demostración: Si x e y son racionales entonces existen enteros a, b, c y d, b y d no nulos, tales que $x = \frac{a}{b}$ e $y = \frac{c}{d}$. Como $a.d + c.b \in \mathbb{Z}$ y $b.d \in \mathbb{Z}$ es no nulo, entonces $\frac{a.d+c.b}{b.d} \in \mathbb{Q}$. Resulta que $\frac{a.d+c.b}{b.d} = (a.d + c.b).(b.d)^{-1} = a.d.(b.d)^{-1} + c.d.(b.d)^{-1} = a.d.b^{-1}.d^{-1} + c.d.b^{-1}.d^{-1} = a.b^{-1} + c.b^{-1} = \frac{a}{b} + \frac{c}{d} = x + y \in \mathbb{Q}$ como queríamos probar. En forma análoga se prueba para el producto. □

Proposición 167. *Si $x \in \mathbb{Q}$ y $x \neq 0$, entonces $x^{-1} \in \mathbb{Q}$.*

Demostración: trivial. □

Observar que $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$. Es claro que $\mathbb{N}$ es un subconjunto propio de $\mathbb{Z}$. A su vez $\mathbb{Z}$ es un subconjunto propio de $\mathbb{Q}$, por ejemplo $\frac{1}{2} \in \mathbb{Q} - \mathbb{Z}$, porque si fuera $k = \frac{1}{2} \in \mathbb{Z}$, entonces $2.k = 2.\frac{1}{2} = 1$; lo cual contradice que los únicos divisores de 1 son 1 y -1. Para probar que $\mathbb{Q}$ es un subconjunto propio de $\mathbb{R}$, debemos asumir un nuevo axioma válido sobre los números reales. Todos los axiomas listados al comienzo del capítulo 3 también se satisfacen en el conjunto de los números racionales.

Axioma de completitud de $\mathbb{R}$: Todo subconjunto no vacío y acotado inferiormente de $\mathbb{R}$ tiene ínfimo. O equivalentemente, todo subconjunto no vacío y acotado superiormente de $\mathbb{R}$ tiene supremo.

Proposición 168. *Si $x \in \mathbb{R}$ entonces existe $n \in \mathbb{N}$ tal que $x < n$.*

Demostración: Supongamos que el enunciado no es cierto, entonces existe $x \in \mathbb{R}$ tal que para todo $n \in \mathbb{N}$ se verifica que $n \leq x$. Resulta $\mathbb{N}$ es un subconjunto no vacío acotado superiormente de $\mathbb{R}$; luego $\mathbb{N}$ tiene supremo, sea a. Como $a - 1 < a$, tenemos que $a - 1$ no es cota superior de $\mathbb{N}$, luego existe $m \in \mathbb{N}$ tal que $a - 1 < m$. Resulta $a < a + 1 = (a - 1) + 2 < m + 2 \in \mathbb{N}$ contradiciendo que a es supremo de $\mathbb{N}$. □

Corolario 169. *Si $x \in \mathbb{R}$ y $x > 0$ entonces existe $n \in \mathbb{N}$ tal que $0 < \frac{1}{n} < x$.*

Demostración: Por la proposición anterior existe $n \in \mathbb{N}$ tal que $x^{-1} < n$. □

El siguiente teorema pueba que el conjunto de los números racionales es **denso** en $\mathbb{R}$; esto significa que los racionales están *por todas partes* en el conjunto de los reales; en otras palabras: dados dos reales cualesquiera, distintos entre sí, no importa cuan cerca esté uno de otro, entre ellos hay algún número racional; más aún, entre ellos hay una cantidad infinita de números racionales.

Teorema 170. *$\mathbb{Q}$ es denso en $\mathbb{R}$, es decir, si x e y son números reales tales que $x < y$ entonces existe $q \in \mathbb{Q}$ tal que $x < q < y$.*

Demostración: Vamos a considerar tres casos: i) $x = 0$, ii) $x > 0$ y iii) $x < 0$.
Caso i): Como $0 = x < y$, por Corolario 169 existe $n_0 \in \mathbb{N}$ tal que $0 < \frac{1}{n_0} < y$.
Caso ii): si $0 < x < y$ entonces $0 < y - x$, luego por Corolario 169 existe $n_0 \in \mathbb{N}$ tal que

$$0 < \tfrac{1}{n_0} < y - x. \tag{4.2}$$

Ahora, $S = \{m \in \mathbb{N} : n_0.x < m\}$ es un subconjunto de $\mathbb{N}$. Por Teorema 168, S es no vacío, entonces existe m_0 primer elemento de S. Resulta que

$$m_0 \in \mathbb{N} \text{ y } n_0.x < m_0. \tag{4.3}$$

Veamos que el racional $q = \frac{m_0}{n_0}$ satisface $x < q < y$. Que $x < \frac{m_0}{n_0}$ resulta directamente de (4.3).
Para probar $\frac{m_0}{n_0} < y$, procedemos por el absurdo: supongamos

$$y \leq \tfrac{m_0}{n_0}. \tag{4.4}$$

$$\begin{aligned} y \leq \tfrac{m_0}{n_0} \quad &\rightarrow \quad y - x \leq \tfrac{m_0}{n_0} - x \\ &\rightarrow \quad 0 < \tfrac{1}{n_0} < y - x \leq \tfrac{m_0}{n_0} - x \quad \text{por (4.2)} \\ &\rightarrow \quad \tfrac{1}{n_0} < \tfrac{m_0}{n_0} - x \\ &\rightarrow \quad x.n_0 < m_0 - 1. \qquad (*) \end{aligned}$$

Observar que si $m_0 - 1 \in \mathbb{N}$ entonces, por (*), $m_0 - 1 \in S$, lo cual contradice que m_0 es el primer elemento de S. Resulta que $m_0 - 1 \notin \mathbb{N}$, luego $m_0 = 1$.
Ahora, nuevamente por (*), tenemos que $x.n_0 < m_0 - 1 = 1 - 1 = 0$, lo cual es absurdo pues $0 < x$ y $n_0 \in \mathbb{N}$.
Hemos probado que $\frac{m_0}{n_0} < y$.
Caso iii): se deduce fácilmente de los casos anteriores. □

Finalmente probaremos que $\mathbb{Q} \neq \mathbb{R}$, es decir, probaremos que $\mathbb{Q}$ es un subconjunto propio de $\mathbb{R}$. Para ello primero veremos que existe un número real cuyo cuadrado es 2, en otras palabras probaremos la existencia del número real $\sqrt{2}$.

Proposición 171. *Existe $s \in \mathbb{R}$ tal que $s^2 = 2$.*

Demostración: Sea $A = \{x \in \mathbb{R} : x^2 \leq 2\}$. Observar que $1 \in A$, luego A es no vacío. Además, A está acotado superiormente, por ejemplo 2 es cota superior; resulta, por el axioma de completitud, que A admite supremo, sea $s \in \mathbb{R}$. Veremos que $s^2 = 2$.
Si $s^2 < 2$, entonces $\frac{2-s^2}{1+2s} > 0$. Luego, por el Corolario 169, existe $a \in \mathbb{R}$, $0 < a < 1$, tal que $0 < a^2 < a < \frac{2-s^2}{1+2s}$. Resulta $2 - s^2 > a.(1 + 2.s) = a + 2.a.s$, de donde $2 > a + 2.a.s + s^2 = (a + s)^2$. Esto implica que $a + s \in A$. Como s es el supremo de A tenemos $a + s \leq s$, luego $a \leq 0$, contradiciendo que $a > 0$.
Si $s^2 > 2$, entonces $\frac{s^2-2}{2.s} > 0$. Luego, por el Corolario 169, existe $a \in \mathbb{R}$, $0 < a < 1$, tal que $0 < a^2 < a < \frac{s^2-2}{2s}$, entonces $s^2 - 2 > 2.a.s > 2.a.s - a^2$, de donde

$$2 < s^2 - 2.a.s + a^2 = (s - a)^2. \tag{4.5}$$

Por otra parte, $a < \frac{s^2-2}{2.s} = \frac{s}{2} - \frac{1}{s} < \frac{s}{2} < s$, entonces $0 < s - a < s$. Como s es el primer elemento de las cotas superiores de A, resulta que $s - a$ no es cota superior de A, es decir, existe $x \in A$ tal que $s - a < x$, luego $(s - a)^2 < x^2 < 2$, lo cual contradice (4.5).
Concluimos que $s^2 = 2$. Además s es el único número real positivo cuyo cuadrado es 2, pues si s' es un real positivo y $s'^2 = 2$ entonces $s^2 - s'^2 = 0$, de donde $(s - s').(s + s') = 0$, resulta $s = s'$ o $s = -s'$, pero como ambos son positivos tenemos que $s = s'$. □

Ejercicio 172. Probar que $\sqrt{2} \notin \mathbb{Q}$. ♢

La Proposición 171 es generalizada por el siguiente teorema. Omitiremos la demostración, es similar a la de dicha proposición.
En adelante indicaremos con $\mathbb{R}^+$ al conjunto de los números reales positivos, es decir, $\mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\}$.

Teorema 173. *Si $x \in \mathbb{R}^+$ y $n \in \mathbb{N}$ entonces existe un único $y \in \mathbb{R}^+$ tal que $y^n = x$, este elemento y se llama **raíz n-ésima** de x y se denota $\sqrt[n]{x}$.*

Sea a un real positivo, $m \in \mathbb{Z}$ y $n \in \mathbb{N}$. Se define la **potencia con exponente racional** $\frac{m}{n}$ de a en la forma: $a^{\frac{m}{n}} = \sqrt[n]{a^m}$.

Veamos que la potencia está bien definida, es decir, si $\frac{m}{n} = \frac{m'}{n'}$ entonces $a^{\frac{m}{n}} = a^{\frac{m'}{n'}}$. Llamemos $x = a^{\frac{m}{n}} = \sqrt[n]{a^m}$. Por definición x es el único número real positivo tal que $x^n = a^m$, entonces, elevando a la m', resulta que $(x^n)^{m'} = (a^m)^{m'}$. Como todos los exponenetes son números enteros, por propiedades probadas para la potenciación con exponentes enteros de números reales, vale que $x^{n.m'} = a^{m.m'}$. Como por hipótesis $n.m' = m.n'$, resulta $x^{m.n'} = a^{m.m'}$ y así $(x^{n'})^m = (a^{m'})^m$, de donde $x^{n'} = a^{m'}$. Resulta que x debe ser el único número real positivo que elevado a la n' da $a^{m'}$, es decir $x = \sqrt[n']{a^{m'}} = a^{\frac{m'}{n'}}$, como queríamos probar.

Las propiedades conocidas para la potencias con exponentes enteros de números reales se extienden para el caso de pontencias racionales, esto es:

Ejercicio 174. Sean a y b reales positivos; q y q' racionales. Probar que:

1. $a^q.a^{q'} = a^{q+q'}$.
2. $\frac{a^q}{a^{q'}} = a^{q-q'}$.
3. $(a^q)^{q'} = a^{q \cdot q'}$.
4. $(a.b)^q = a^q.b^q$.
5. $(\frac{a}{b})^q = \frac{a^q}{b^q}$. ♢

Observar que cuando $q = \frac{1}{n}, q' = \frac{1}{n'}$, con n y n' números naturales, de las propiedades probadas en el ejercicio anterior resulta que:

1. $\sqrt[n]{a}. \sqrt[n']{a} = \sqrt[n.n']{a^{n+n'}}$.
2. $\frac{\sqrt[n]{a}}{\sqrt[n']{a}} = \sqrt[n.n']{a^{n-n'}}$.
3. $\sqrt[n]{\sqrt[n']{a}} = \sqrt[n.n']{a}$.

Se llama número **irracional** a todo número real no racional, es decir, el conjunto de los números irracionales se define como $\mathbb{I} = \mathbb{R} - \mathbb{Q}$.

Las operaciones suma + y producto . no son cerradas en $\mathbb{I}$, por ejemplo, $\sqrt{2}$ y $-\sqrt{2}$ son números irracionales, pero $\sqrt{2} + (-\sqrt{2}) = 0$ no es irracional y $\sqrt{2}.(-\sqrt{2}) = -2$ no es irracional.

Ejercicio 175. Probar que

Si $x \in \mathbb{I}$ y $q \in \mathbb{Q}$ entonces $x + q \in \mathbb{I}$.

Si $x \in \mathbb{I}$, $0 \neq q$ y $q \in \mathbb{Q}$ entonces $x.q \in \mathbb{I}$.

En particular, si $x \in \mathbb{I}$ entonces $-x \in \mathbb{I}$ y $x^{-1} \in \mathbb{I}$.

Además $\mathbb{I}$ es denso en $\mathbb{R}$, es decir:

Si x e y son reales y $x < y$ entonces existe $z \in \mathbb{I}$ tal que $x < z < y$. $\diamondsuit$

Capítulo 5

Números complejos

5.1. Forma de par ordenado. Operaciones. Forma binómica

Un número **complejo** es un par ordenado cuyas componentes son números reales. Luego el conjunto de los números complejos es

$$\mathbb{C} = \{(x, y) : x \in \mathbb{R} \wedge y \in \mathbb{R}\}.$$

Si $z = (a, b) \in \mathbb{C}$, la primer componente a se dice la **parte real** de z y la segunda componente b se dice la **parte imaginaria** de z, lo cual se indica respectivamente

$$Re(z) = a \quad \text{y} \quad Im(z) = b.$$

Se define en $\mathbb{C}$ una operación suma $+$ y una operación producto $.$, en la forma: para $z_1 = (a_1, b_1)$ y $z_2 = (a_2, b_2)$ complejos cualesquiera se tiene que

$$z_1 + z_2 = (a_1 + a_2, b_1 + b_2);$$

$$z_1.z_2 = (a_1.a_2 - b_1.b_2, a_1.b_2 + b_1.a_2),$$

donde las operaciones indicadas entre las componentes de z_1 y z_2 son las operaciones suma y producto de números reales estudiadas en los capítulos anteriores; es claro entonces que $z_1 + z_2 \in \mathbb{C}$ y que $z_1.z_2 \in \mathbb{C}$.

Ejemplo 176.

Si $z_1 = (2, 3)$, $z_2 = (-1, 4)$, $z_3 = (2, 0)$ y $z_4 = (0, 1)$ entonces

$z_1 + z_2 = (2 + (-1), 3 + 4) = (1, 7);$

$z_1.z_2 = (2.(-1) - 3.4, 2.4 + 3.(-1)) = (-14, 5);$

$z_3.z_4 = (2.0 - 0.1, 2.1 + 0.0) = (0, 2);$

$z_4.z_4 = (0.0 - 1.1, 1.0 + 0.1) = (-1, 0).$



Proposición 177. *La suma y el producto de números complejos satisfacen las mismas propiedades que la suma y el producto de números reales:*

1. *La suma y el producto son operaciones* ***asociativas****, es decir, dados complejos cualesquiera z_1, z_2 y z_3 se satisface que*

$$(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3);$$

$$(z_1.z_2).z_3 = z_1.(z_2.z_3).$$

2. *La suma y el producto son operaciones* ***conmutativas****, es decir, dados complejos cualesquiera z_1 y z_2 se satisface que*

$$z_1 + z_2 = z_2 + z_1;$$

$$z_1.z_2 = z_2.z_1.$$

3. *El número complejo $(0, 0)$ es el* ***neutro de la suma****, es decir, para todo complejo z se satisface que*

$$z + (0, 0) = z.$$

El número complejo $(1, 0)$ es el ***neutro del producto****, es decir, para todo complejo z se satisface que*

$$z.(1, 0) = z.$$

4. *Todo número complejo admite un* ***opuesto según la suma****, es decir, dado un número complejo z cualquiera, existe un único número complejo, que se denota $-z$, tal que $z + (-z) = 0$.*

5. *Todo número complejo no nulo admite un* ***inverso según el producto****, es decir, dado un número complejo z cualquiera, $z \neq (0,0)$, existe un único número complejo, que se denota z^{-1}, tal que $z.z^{-1} = (1,0)$.*
6. *El producto es distributivo con respecto a la suma, es decir, dados complejos cualesquiera z_1, z_2 y z_3 se satisface que*

$$z_1.(z_2 + z_3) = z_1.z_2 + z_1.z_3.$$

Demostración: Demostraremos algunas de las propiedades enunciadas, las restantes demostraciones quedan como ejercicios.

1) Sea $z_1 = (a_1, b_1)$, $z_2 = (a_2, b_2)$ y $z_3 = (a_3, b_3)$, luego $(z_1 + z_2) + z_3 = ((a_1, b_1) + (a_2, b_2)) + (a_3, b_3) = (a_1 + a_2, b_1 + b_2) + (a_3, b_3) = ((a_1 + a_2) + a_3, (b_1 + b_2) + b_3)$.

Como la suma de número reales es asociativa, sabemos que $(a_1+a_2)+a_3 = a_1+(a_2+a_3)$ y $(b_1 + b_2) + b_3 = b_1 + (b_2 + b_3)$.

Luego $((a_1 + a_2) + a_3, (b_1 + b_2) + b_3) = (a_1 + (a_2 + a_3), b_1 + (b_2 + b_3)) = (a_1, b_1) + (a_2 + a_3, b_2 + b_3) = (a_1, b_1) + ((a_2, b_2) + (a_3, b_3)) = z_1 + (z_2 + z_3)$ como queríamos probar.

4) Sea $z = (a, b)$ un complejo cualquiera; como a y b son números reales, sabemos que existen números reales $-a$ y $-b$ tales que $a + (-a) = 0$ y $b + (-b) = 0$. Luego $(-a, -b) \in \mathbb{C}$ y $(a, b) + (-a, -b) = (a + (-a), b + (-b)) = (0, 0)$. Resulta que $-z = (-a, -b)$.

5) Sea $z = (a, b)$ un complejo cualquiera no nulo, luego $a^2+b^2 \neq 0$, de donde $\frac{a}{a^2+b^2} \in \mathbb{R}$ y $\frac{-b}{a^2+b^2} \in \mathbb{R}$. Resulta que $(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}) \in \mathbb{C}$ y
$(a, b).(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}) = (a.\frac{a}{a^2+b^2} - b.\frac{(-b)}{a^2+b^2}, a.\frac{(-b)}{a^2+b^2} + b.\frac{a}{a^2+b^2}) = (1, 0)$; concluimos que $z^{-1} = (\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$, como queríamos probar. Supongamos existe otro complejo w tal que $z.w = (1, 0)$, entonces, usando que $(1, 0)$ es neutro para el producto,

$$z^{-1} = z^{-1}.(1, 0) = z^{-1}.(z.w) = (z^{-1}.z).w = (1, 0).w = w.$$

□

Convención: Como en el caso de los números reales, para simplificar la notación, podemos escribir:

- $z_1 - z_2$ en lugar de $z_1 + (-z_2)$;
- $\frac{1}{z}$ en lugar de z^{-1};

- $\frac{z_1}{z_2}$ en lugar de $z_1.z_2^{-1}$

Los números reales se **identifican** con los números complejos con parte imaginaria nula, es decir, cada número real a se identifica con el número complejo $(a, 0)$. Esta identificación es *buena* en el sentido que *respeta* las operaciones suma y producto. En otras palabras, sumar o multiplicar en $\mathbb{R}$ a dos números reales a_1 y a_2 es quivalente a sumar o multiplicar en $\mathbb{C}$ los correspondientes números complejos $(a_1, 0)$ y $(a_2, 0)$. Efectivamente, $(a_1, 0) + (a_2, 0) = (a_1 + a_2, 0)$ y $(a_1, 0).(a_2, 0) = (a_1.a_2, 0)$.
En consecuencia convendremos en escribir al número complejo $(a, 0)$ simplemente como a. Observar que el complejo nulo $(0, 0)$ se representa por 0.
Un complejo se dice **imaginario puro** si su parte real es 0. Llamamos **unidad imaginaria** al complejo $(0, 1)$ y lo representamos por i. Luego, un complejo imaginario puro $(0, b)$ es igual a $b.i$ pues de acuerdo a lo convenido $b.i = (b, 0).(0, 1) = (0, b)$. Observar que $0.i = (0, 0).(0, 1) = (0, 0) = 0$. Por otra parte, $i.i = (0, 1).(0, 1) = (-1, 0) = -1$.
Dicho todo esto resulta que un complejo cualquiera $z = (a, b)$ se puede escribir como $z = (a, b) = (a, 0) + (0, b) = a + b.i$. Esta forma de escribir a un número complejo se llama **forma binómica** y es útil para simplificar la escritura y facilitar los cálculos. Algunas veces también escribiremos $a + bi$ en lugar de $a + b.i$. Tenemos así que

$$\mathbb{C} = \{a + bi \text{ con } a \in \mathbb{R} \text{ y } b \in \mathbb{R}\}.$$

Trabajando en forma binómica, las operaciones suma y producto y los inversos aditivos y multiplicativos se expresan de la siguiente manera:

$$(a + bi) + (c + di) = (a + c) + (b + d)i;$$

$$(a + bi).(c + di) = (a.c - b.d) + (b.c + a.d)i;$$

$$-(a + bi) = -a - bi;$$

$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} + (\frac{-b}{a^2 + b^2})i.$$

Ejemplo 178.

- Sean $z = 3 + 2i$ y $w = -1 - 4i$, tenemos que

  $5.z = 5.(3 + 2i) = 15 + 10i$

  $i.z = i.(3 + 2i) = i.3 + i.2.i = 3.i + 2.(-1) = -2 + 3i$

  $z + w = 2 - 2i$

  $8.(z - 1) + w.z - 3i = 8.(3 + 2i - 1) + (-1 - 4i).(3 + 2i) - 3i =$

  $= 16 + 16i - 3 - 2i - 12i + 8 - 3i = 21 - i.$
- $\frac{(3+2i).(-2+i)}{5i(4-i)} = \frac{-6+3i-4i+2i^2}{20i-5i^2} = \frac{-6-i-2}{20i+5} = (-8 - i).(5 + 20i)^{-1} =$
  $= (-8 - i).(\frac{5}{\sqrt{425}} - \frac{20}{\sqrt{425}}i) = -8.\frac{5}{\sqrt{425}} + 8.\frac{20}{\sqrt{425}}i - \frac{5}{\sqrt{425}}i + \frac{20}{\sqrt{425}}i^2 =$
  $-\frac{60}{\sqrt{425}} + \frac{155}{\sqrt{425}}i = -\frac{12}{\sqrt{17}} + \frac{31}{\sqrt{17}}i.$ ♢

Como en el caso de los números reales se define la potencia con exponente entero m de un número complejo z en la forma

$$z^m = \begin{cases} z & \text{si } m = 1; \\ z.z^{m-1} & \text{si } m > 1; \\ 1 & \text{si } m = 0 \text{ y } z \neq 0; \\ (z^{-1})^{|m|} & \text{si } m < 0. \end{cases}$$

Ejemplo 179.

$i^2 = i.i = -1 \quad i^3 = i^2.i = (-1).i = -i$

$i^4 = i^3.i = (-i).i = -(i.i) = -(-1) = 1 \quad i^5 = i^4.i = 1.i = i.$

$(3 + 2i)^2 = (3 + 2i).(3 + 2i) = (9 - 4) + (6 + 6)i = 5 + 12i.$ ♢

Proposición 180. *Si z y w son complejos no nulos y n y m son enteros entonces*

- $(z.w)^n = z^n.w^n$
- $(\frac{z}{w})^n = \frac{z^n}{w^n}$
- $(z^n)^m = z^{n.m}$
- $z^n.z^m = z^{n+m}$
- $\frac{z^n}{z^m} = z^{n-m}$

Demostración: Se deja como ejercicio. □

Observar que si $n \in \mathbb{N}$, por el algoritmo de la división existe $k \in \mathbb{N}$ tal que $n = k.4 + r_4(n)$, luego $i^n = i^{k.4+r_4(n)} = i^{k.4}.i^{r_4(n)} = (i^4)^k.i^{r_4(n)} = 1^k.i^{r_4(n)} = i^{r_4(n)}$.

Ejercicio 181.

Probar que si $z = a + bi$ y $n \in \mathbb{N}$ entonces

$$z^n = (a+bi)^n = \sum_{j=0}^{n} \left(\begin{array}{c} n \\ j \end{array} \right) a^{n-j}.b^j.i^j$$

En particular

$(a+bi)^2 = a^2 + 2abi + b^2i^2 = a^2 - b^2 + 2abi.$

$(a+bi)^3 = a^3+3a^2bi+3ab^2i^2+b^3i^3 = a^3+3a^2bi-3ab^2-b^3i = (a^3-3ab^2)+(3a^2b-b^3)i$♢

Sea $z = a + bi$ con $a, b \in \mathbb{R}$. Se llama **conjugado** de z al número complejo que se denota $\overline{z}$ dado por $\overline{z} = a - bi$.

Ejemplo 182.

$(3+i)^2 - 2i = 9 - 6i + i^2 - 2i = 9 - 6i - 1 - 2i = 8 - 8i.$

Si $z = 5 - 4i$ entonces $\overline{z} = 5 + 4i.$

Si $z = 10$ entonces $\overline{z} = 10.$

Si $z = \sqrt{3}i$ entonces $\overline{z} = -\sqrt{3}\,i.$ ♢

Proposición 183. *Si z y w son complejos entonces*

1. $\overline{\overline{z}} = z.$
2. $\overline{z+w} = \overline{z} + \overline{w}$ *y* $\overline{z.w} = \overline{z}.\overline{w}.$
3. $\overline{z^{-1}} = (\overline{z})^{-1}$*; luego,* $\overline{\left(\frac{w}{z}\right)} = \frac{\overline{w}}{\overline{z}}.$
4. $(\overline{z})^n = \overline{z^n}$ *para todo* $n \in \mathbb{N}.$
5. $z + \overline{z} = 2.Re(z)$ *y* $z - \overline{z} = 2.Im(z).i.$

Demostración: 1., 2. y 5. son triviales.

Veamos 3.: por 2. tenemos que $\overline{z}.\overline{z^{-1}} = \overline{z.z^{-1}} = \overline{1} = 1$; luego, por la unicidad del inverso multiplicativo, $(\overline{z})^{-1} = \overline{z^{-1}}$ como queríamos probar.

El item 4. se prueba facilmente por inducción en n. □

Sea $z = a + bi$ con $a, b \in \mathbb{R}$. Se llama **módulo** de z al número real no negativo, que se denota $\mid z \mid$, dado por $\mid z \mid = \sqrt{a^2 + b^2}$.

Ejemplo 184.

$\mid 3 - 2i \mid = \sqrt{3^2 + (-2)^2} = \sqrt{9+4} = \sqrt{13}$

$\mid i \mid = \sqrt{0^2 + 1^2} = \sqrt{1} = 1$

$\mid -8 \mid = \sqrt{(-8)^2 + 0^2} = \sqrt{(-8)^2} = 8$

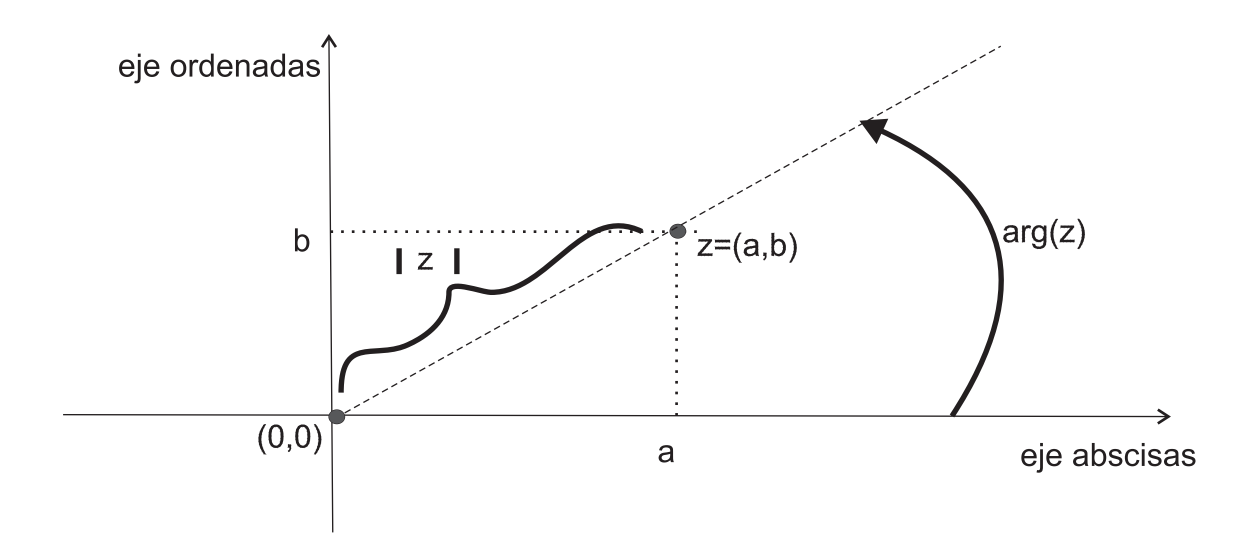


Figura 5.1: módulo y argumento de un número complejo.

Observar que el módulo de un numero complejo $z = a + 0i$ con parte imaginaria nula coincide con el módulo del número real a definido en los capítulos anteriores. $\diamondsuit$

Proposición 185. *Dados números complejos z y w se satisface que*

1. $\mid z \mid = 0 \leftrightarrow z = 0$.
2. $\mid z.w \mid = \mid z \mid . \mid w \mid$.
3. $\mid \overline{z} \mid = \mid z \mid$.
4. $z.\overline{z} = \mid z \mid^2$.
5. $\mid z \mid^n = \mid z^n \mid$ *para todo* $n \in \mathbb{N}$.
6. $\mid z + w \mid \leq \mid z \mid + \mid w \mid$, *esta relación se llama desigualdad triangular.*

Demostración: Los items 1.,2.,3. y 4. se prueban facilmente mediante cálculo directo a partir de la forma binómica. El item 5. también es fácil de probar por inducción en n.

Veamos 6.: como $\mid z + w \mid$ y $\mid z \mid + \mid w \mid$ son reales positivos, es suficiente probar que $\mid z + w \mid^2 \leq (\mid z \mid + \mid w \mid)^2$. Usando 4. tenemos que

$$\mid z + w \mid^2 = (z + w).(\overline{z + w}) = (z + w).(\overline{z} + \overline{w}) = \mid z \mid^2 + z.\overline{w} + w.\overline{z} + \mid w \mid^2 .$$

Observando que

$$z.\overline{w} + w.\overline{z} = z.\overline{w} + \overline{\overline{w}.z} = z.\overline{w} + \overline{z.\overline{w}} = 2.Re(z.\overline{w}) \leq 2. \mid z.\overline{w} \mid = 2. \mid z \mid . \mid w \mid,$$

obtenemos

$$| z + w |^2 \leq | z |^2 + 2. | z | . | w | + | w |^2 = (| z | + | w |)^2,$$

como queríamos probar. □

5.2. Forma trigonométrica

Así como los números reales se corresponde con los puntos de una recta, los números complejos se corresponden con los puntos de un plano. Si fijamos en el plano un par de **ejes coordenados** perpendiculares entre sí, el primero se llama **eje de abscisas** y el segundo **eje de ordenadas**, cada punto del plano está unívocamente determinado por un par de coordenadas (a, b). Como cada par (a, b) se corresponde con un único número complejo, podemos asignar en forma biyectiva a cada punto del plano un número complejo. Ver Figura 5.1.

Ejemplo 186.

Las regiones del plano sombreadas en la Figura 5.2 se corresponden con los siguientes subconjuntos de $\mathbb{C}$:

$A = \{z \in \mathbb{C} : Re(z) = 1\};$

$B = \{z \in \mathbb{C} : Re(z) \leq -3\};$

$C = \{z \in \mathbb{C} : Re(z) + Im(z) \geq 2\}.$ ♢

Dado un número complejo $z = a + bi$ su módulo $| z |= \sqrt{a^2 + b^2}$ es exactamente la distancia entre el origen $(0, 0)$ y el punto (a, b). Más aún, si $z_0 = a_0 + b_0 i$ entonces $| z - z_0 |=| (a - a_0) + (b - b_0)i |= \sqrt{(a - a_0)^2 + (b - b_0)^2}$ es la distancia entre el punto (a_0, b_0) y el punto (a, b). Ver Figura 5.1.

Ejemplo 187.

Las regiones del plano sombreadas en la Figura 5.3 se corresponden con los siguientes subconjuntos de $\mathbb{C}$:

$D = \{z \in \mathbb{C} :| z |= 1\};$

$E = \{z \in \mathbb{C} : Im(z) \geq 2 \wedge \ | z |\leq 6\};$

$F = \{z \in \mathbb{C} :| z - (2 + 3i) |\leq 4\}.$ ♢

Dado un complejo $z = a + bi$ no nulo, el ángulo barrido por el semieje de abscisas positivas al desplazarse en sentido antihorario hasta la semirrecta con origen en $(0, 0)$ que contiene al punto (a, b) se llama **argumento principal** de z y se indica $arg(z)$.

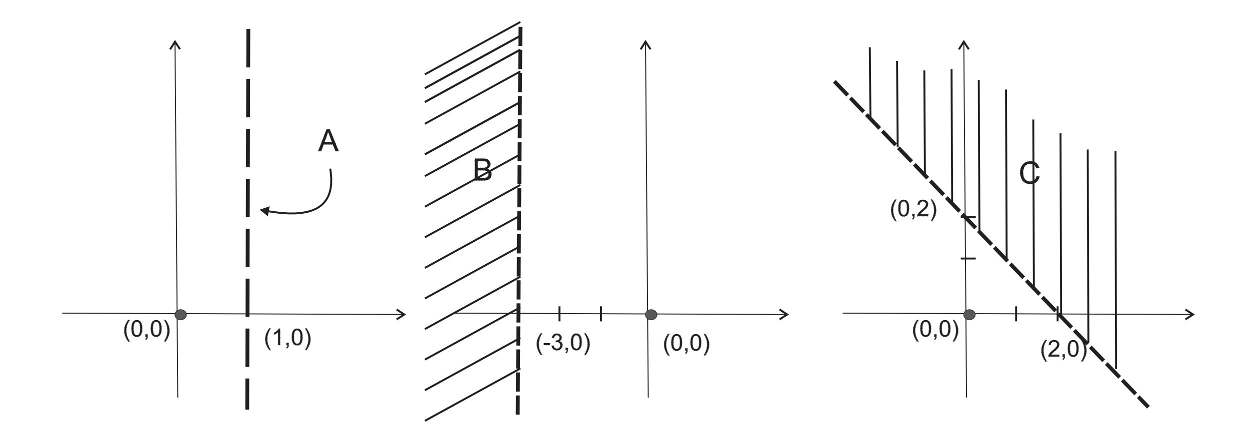


Figura 5.2: ver Ejemplo 186.

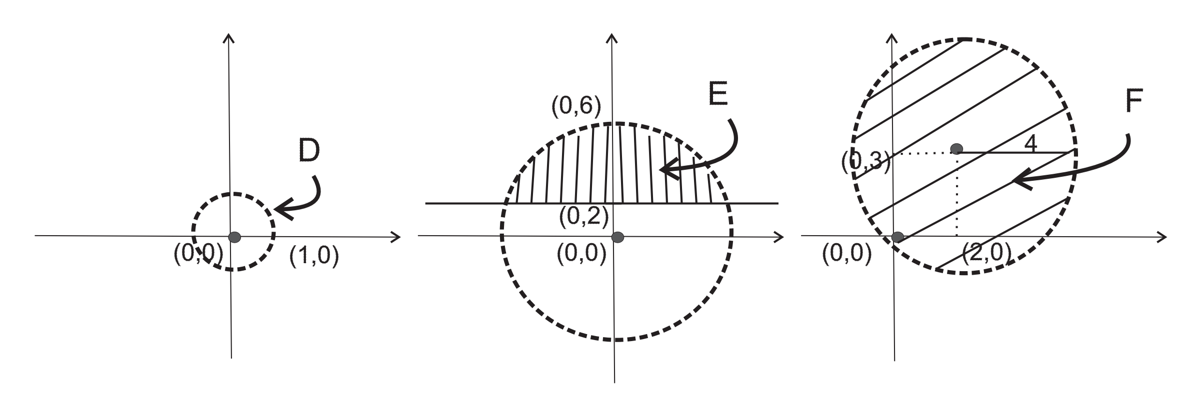


Figura 5.3: ver Ejemplo 187.

Observar que $0 \leq arg(z) < 2\pi$. No definimos argumento del complezo $z = 0$. Ver Figura 5.1.

Ejemplo 188.

- Las regiones del plano sombreadas en la Figura 5.4 se corresponden con los siguientes subconjuntos de $\mathbb{C}$:
  $G = \{z \in \mathbb{C} : 0 \leq arg(z) \leq \frac{\pi}{4}\}$
  $H = \{z \in \mathbb{C} : \frac{\pi}{4} \leq arg(z) \leq \pi \wedge Re(z) \geq -1\}$
- Sea $z_0 = 3 + 3i$. Tenemos que $| z_0 |= \sqrt{3^2 + 3^2} = \sqrt{18}$ y $arg(z_0) = \frac{\pi}{4}$. Observar que existen infinitos números complejos cuyo módulo es $\sqrt{18}$: todos los que se corresponden con los puntos de la circuferencia centrada en $(0,0)$ con radio $\sqrt{18}$. Y existen infinitos números complejos cuyo argumento principal es igual a $\frac{\pi}{4}$: todo los pertenecientes a la semirrecta bisectriz del primer cuadrante. Pero $3+3i$ es el único número complejo cuyo módulo es $\sqrt{18}$ y su argumento es $\frac{\pi}{4}$.$\diamondsuit$

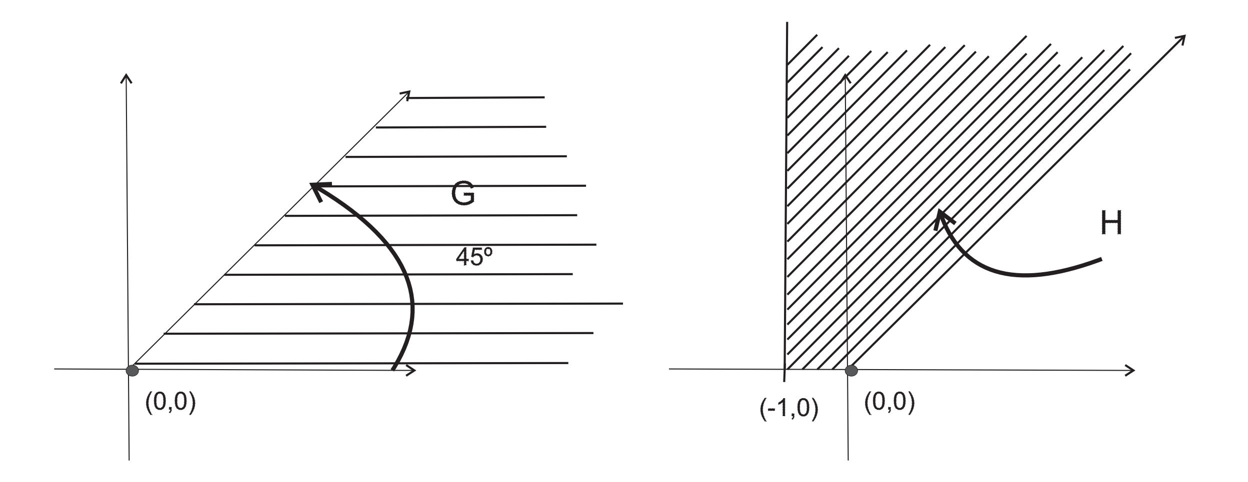


Figura 5.4: ver Ejemplo 188.

Todo número complejo queda determinado por su módulo y su argumento principal. Observar que:

z es un real positivo $\leftrightarrow arg(z) = 0$.

z es un real negativo $\leftrightarrow arg(z) = \pi$.

z es un imaginario puro con $Im(z) > 0 \leftrightarrow arg(z) = \frac{\pi}{2}$.

z es un imaginario puro con $Im(z) < 0 \leftrightarrow arg(z) = \frac{3\pi}{2}$.

Por otra parte, si $z = a + bi$ con a y b reales no nulos entonces (a, b) es un punto del plano contenido en el interior de uno de los cuatro cuadrantes, a saber:

en el **primer cuadrante** si $a > 0$ y $b > 0$;
en el **segundo cuadrante** si $a < 0$ y $b > 0$;
en el **tercer cuadrante** si $a < 0$ y $b < 0$; y
en el **cuarto cuadrante** si $a > 0$ y $b < 0$.

En cualquier caso, como $tangente(arg(z)) = \frac{b}{a}$, tenemos que

$$arg(z) = \begin{cases} arctan(\mid \frac{b}{a} \mid), & \text{si } z \text{ está en el primer cuadrante;} \\ \pi - arctan(\mid \frac{b}{a} \mid), & \text{si } z \text{ está en el segundo cuadrante;} \\ \pi + arctan(\mid \frac{b}{a} \mid), & \text{si } z \text{ está en el tercer cuadrante; y} \\ 2\pi - arctan(\mid \frac{b}{a} \mid), & \text{si } z \text{ está en el cuarto cuadrante;} \end{cases}$$

donde $arctan : \mathbb{R} \to (-\frac{\pi}{2}, \frac{\pi}{2})$ es la función inversa de la función trigonométrica *tangente* restringida al intervalo $(-\frac{\pi}{2}, \frac{\pi}{2})$.

Ejemplo 189.

Recordando que

α	0	$\frac{\pi}{12}$	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$
$tangente(\alpha)$	0	$2-\sqrt{3}$	$\frac{1}{\sqrt{3}}$	1	$\sqrt{3}$

tenemos que

$arg(1+\sqrt{3}\,i) = arctan(\frac{\sqrt{3}}{1}) = \frac{\pi}{3}$.

$arg(5-5\,i) = 2.\pi - arctan(\frac{5}{5}) = 2.\pi - arctan(1) = 2.\pi - \frac{\pi}{4} = \frac{7}{4}.\pi$.

$arg(-2.\sqrt{3}-2\,i) = \pi + arctan(\frac{2}{2.\sqrt{3}}) = \pi + arctan(\frac{1}{\sqrt{3}}) = \pi + \frac{\pi}{6} = \frac{7}{6}.\pi$. ♢

Sea $z = a + bi$ no nulo con $a, b \in \mathbb{R}$. Como las funciones seno y coseno son periódicas con período $2.\pi$, si $\alpha = arg(z) + k.2.\pi$ con k es un entero cualquiera entonces

$$cos(\alpha) = cos(arg(z)) = \frac{a}{\mid z \mid};$$

$$sen(\alpha) = sen(arg(z)) = \frac{b}{\mid z \mid}.$$

Resulta que $z = a + bi =\mid z \mid .cos(\alpha) + \mid z \mid .sen(\alpha)\, i;$ luego

$$z = \mid z \mid .(cos(\alpha) + i\, sen(\alpha)).$$

Esta forma de escribir un número complejo se llama **forma trigonométrica**.

Observar que si r y θ son reales cualesquiera con $r > 0$, entonces la forma trigonométrica de $w = r.\,cos(\theta) + r.\,sen(\theta)\,.i$ es

$$r.(cos(\theta) + i\, sen(\theta));$$

pues

$$\mid w \mid = \sqrt{(rcos(\theta))^2 + (rsen(\theta))^2} = \sqrt{r^2(cos^2(\theta) + sen^2(\theta))} = \sqrt{r^2} = \mid r \mid = r;$$

y $\theta = arg(w) + k.2.\pi$ para algún $k \in \mathbb{Z}$ porque

$$\frac{rsen(\theta)}{rcos(\theta)} = \frac{sen(\theta)}{cos(\theta)} = tangente(\theta).$$

Proposición 190. *Si $z = r.\,(cos(\theta) + i\, sen(\theta))$ con $r \in \mathbb{R}^+$ y $\theta \in \mathbb{R}$ entonces*

$$\overline{z} = r.\,(cos(-\theta) + i\, sen(-\theta));$$

$$z^{-1} = \frac{1}{r}.(cos(-\theta) + i\, sen(-\theta)).$$

Demostración: Se deja como ejercicio. □

Proposición 191. *Si* $z_1 = r_1(cos(\theta_1) + i\, sen(\theta_1))$ *y* $z_2 = r_2(cos(\theta_2) + i\, sen(\theta_2))$ *con* $r_1, r_2 \in \mathbb{R}^+$ *y* $\theta_1, \theta_2 \in \mathbb{R}$*, entonces*

$$z_1.z_2 = r_1.r_2\ (cos(\theta_1 + \theta_2) + i\, sen(\theta_1 + \theta_2));$$

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}\ (cos(\theta_1 - \theta_2) + i\, sen(\theta_1 - \theta_2)).$$

Demostración: Operando en forma binómica y recordando las relaciones trigonométricas que establecen que, para α y β cualesquiera,

$$sen(\alpha + \beta) = sen(\alpha).cos(\beta) + cos(\alpha).sen(\beta),$$

$$cos(\alpha + \beta) = cos(\alpha).cos(\beta) - sen(\alpha).sen(\beta),$$

tenemos que

$$z_1.z_2 = (r_1.(cos(\theta_1) + i\, sen(\theta_1))).(r_2.(cos(\theta_2) + i\, sen(\theta_2))) =$$

$$= r_1.r_2.(cos(\theta_1).cos(\theta_2) - sen(\theta_1).sen(\theta_2)) + i\, (sen(\theta_1).cos(\theta_2) + cos(\theta_1).sen(\theta_2)) =$$

$$= r_1.r_2.(cos(\theta_1 + \theta_2) + i\, sen(\theta_1 + \theta_2)).$$

La demostración en el caso del cociente es trivial a partir de la Proposición 190 pues $\frac{z_1}{z_2} = z_1.z_2^{-1}$. □

Proposición 192 (Fórmula de De Moivre)**.** *Si* $z = r.\,(cos(\theta) + i\, sen(\theta))$ *con* $r \in \mathbb{R}^+$ *y* $\theta \in \mathbb{R}$ *entonces, para todo* $m \in \mathbb{Z}$*,*

$$z^m = r^m.\,(cos(m.\theta) + i\, sen(m.\theta)).$$

Demostración: La proposición vale para $m = 0$ pues $z^0 = 1$ y

$$r^0\,.(cos(0.\theta) + i\, sen(0.\theta)) = 1.\,(cos(0) + i\, sen(0)) = 1.$$

Cuando $m \in \mathbb{N}$ se prueba por inducción usando la Proposición 191 en el paso inductivo.
Cuando $m < 0$, usando que la proposición vale para $\mid m \mid$ y la Proposición 190, tenemos que

$z^m = z^{-|m|} = (z^{-1})^{|m|} = (r^{-1}.\,(cos(-\theta) + i\,sen(-\theta)))^{|m|} =$

$= (r^{-1})^{|m|}.\,(cos(\mid m \mid .(-\theta)) + i\,sen(\mid m \mid .(-\theta))) =$

$= r^m\,(cos(m.\theta) + i\,sen(m.\theta)).$

□

Ejemplo 193.

- Calcular $(1+\sqrt{3}\,i)^{31}$. Observar que realizar este cálculo utilizando la forma binómica es muy trabajoso. Operaremos usando la forma trigonométrica.
  Si $z = 1+\sqrt{3}\,i$ entonces $\mid z \mid = \sqrt{1+3} = 2$ y $arg(z) = arctan(\frac{\sqrt{3}}{1}) = \frac{\pi}{3}$; luego $z = 2.(cos(\frac{\pi}{3}) + isen(\frac{\pi}{3})$. Utilizando la fórmula de De Moivre obtenemos que

$$z^{31} = 2^{31}.(cos(31.\frac{\pi}{3}) + isen(31.\frac{\pi}{3})).$$

  Como $\frac{31}{3}.\pi = (10+\frac{1}{3}).\pi = 5.(2.\pi) + \frac{1}{3}.\pi$, resulta

$$z^{31} = 2^{31}(cos(\frac{1}{3}.\pi) + isen(\frac{1}{3}.\pi)) = 2^{31}(\frac{1}{2} + \frac{\sqrt{3}}{2}) = 2^{30} + 2^{30}.\sqrt{3}\,i.$$

- Determinar n tal que $(2+2i)^n$ sea un número real negativo. Como observamos precedentemente, un complejo es un real negativo si y sólo si su argumento es π. Calcularemos el argumento de $(2+2i)^n$.
  Como $2+2i = \sqrt{8}.(cos(\frac{\pi}{4}) + i\,sen(\frac{\pi}{4}))$, por la fórmula de De Moivre,

$$(2+2i)^n = (\sqrt{8})^n.(cos(n.\frac{\pi}{4}) + i\,sen(n.\frac{\pi}{4})).$$

  Resulta que $n.\frac{\pi}{4} = arg((2+2i)^n) + k.2.\pi$ para algún entero k. Concluimos que $(2+2i)^n$ es un real negativo si y sólo si $n.\frac{\pi}{4} - k.2.\pi = \pi$ para algún entero k. Esto ocurre si y sólo si $\frac{n}{4} = 1+2.k$ o equivalentemente si y sólo si $n = 4+8.k$ para algún entero k.
  Resulta que existe una cantidad infinita de soluciones del problema propuesto. Por ejemplo:
  con $k=0$ obtenemos $n=4$: efectivamente $(2+2i)^4 = -64$;
  con $k=1$ obtenemos $n=12$: efectivamente $(2+2i)^{12} = -262144$;
  con $k=-1$ obtenemos $n=-4$: efectivamente $(2+2i)^{-4} = -\frac{1}{64}$. ♢

5.3. Radicación de números complejos

En el Capítulo 4 vimos que dado $a \in \mathbb{R}^+$ y $n \in \mathbb{N}$, existe un único número real positivo cuya potencia n-ésima es igual a a, tal número se llama raíz n-ésima positiva de a y se denota $\sqrt[n]{a}$. Ahora nos planteamos un problema similar en el contexto de los números complejos: dado un número complejo cualquiera z_0 y $n \in \mathbb{N}$ queremos determinar si existe algún número complejo w tal que $w^n = z_0$, en tal caso w se dice una **raíz n-ésima** de z_0; veremos a continuación que todo complejo no nulo tiene exactamente n raíces n-ésimas.

Proposición 194. *Sea $z_0 \in \mathbb{C}$ no nulo y $n \in \mathbb{N}$. Existen exactamente n números complejos w tales que $w^n = z_0$.*

Demostración: Para simplificar la notación llamemos $r_0 =\mid z_0 \mid$ y $\alpha_0 = arg(z_0)$, luego $z_0 = r_0.\,(cos(\alpha_0) + i\,sen(\alpha_0))$.
Queremos determinar si existen complejos $w = r.(cos(\alpha) + isen(\alpha))$ con $r \in \mathbb{R}^+$ y $\alpha \in \mathbb{R}$ tales que $w^n = z_0$. Por la fórmula de De Moivre tenemos

$$w^n = z_0$$

$$\Updownarrow$$

$$r^n\,.(cos(n.\alpha) + i\,sen(n.\alpha)) = r_0.\,(cos(\alpha_0) + i\,sen(\alpha_0))$$

$$\Updownarrow$$

$$\begin{cases} r^n = r_0 \\ n.\alpha = \alpha_0 + k.2.\pi \quad \text{para algún entero } k. \end{cases}$$

$$\Updownarrow$$

$$\begin{cases} r = \sqrt[n]{r_0} \\ \alpha = \frac{\alpha_0}{n} + \frac{k}{n}.2.\pi \quad \text{para algún entero } k. \end{cases}$$

Como las funciones seno y coseno son periódicas con período $2.\pi$ basta considerar k tal que $0 \leq k < n$; así obtenemos las n soluciones de la ecuación planteada:

$$w_k = \sqrt[n]{r_0}.\,(cos(\frac{\alpha_0}{n} + k.\frac{2.\pi}{n}) + i\,sen(\frac{\alpha_0}{n} + k.\frac{2.\pi}{n})$$

para $0 \leq k \leq n-1$. Ver Figura 5.5 □

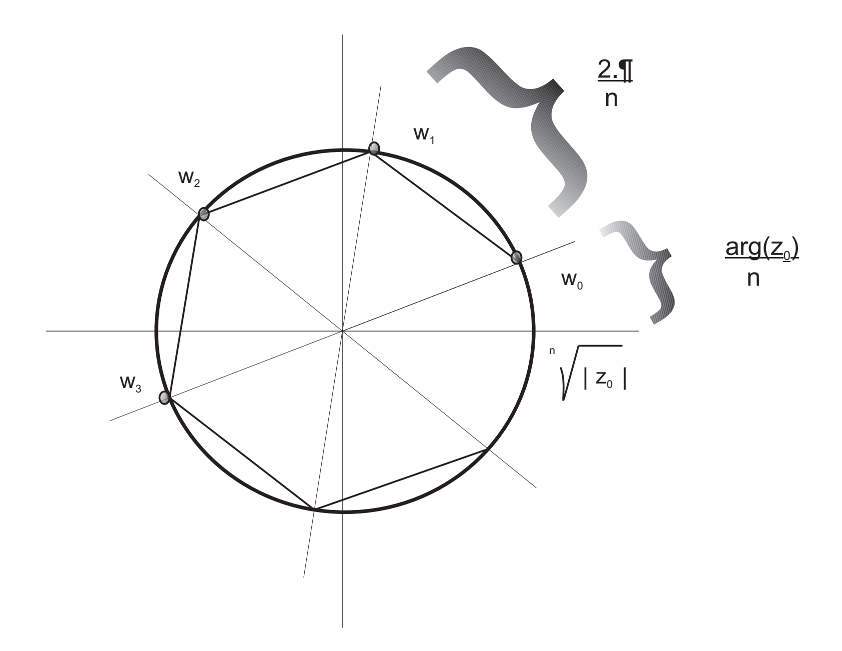


Figura 5.5: las soluciones de $w^n = z_0$ se corresponden con los vértices del polígono regular con n vértices centrado en $(0, 0)$ inscripto en la circunferencia con radio $\sqrt[n]{\mid z_0 \mid}$, es decir, comenzando con w_0 con argumento $\frac{arg(z_0)}{n}$, las restantes raíces se obtienen incrementando el argumento en $\frac{2.\pi}{n}$.

Ejemplo 195.

Determinar las raíces cuartas de $1 + i$, es decir, determinar los complejos w tales que $w^4 = 1 + i$.

Como $\mid 1 + i \mid = \sqrt{2}$ y $arg(1 + i) = \frac{\pi}{4}$, las cuatro raíces cuartas de $1 + i$ son

$$w_0 = \sqrt[4]{\sqrt{2}}.(cos(\tfrac{\pi}{16}) + isen(\tfrac{\pi}{16}));$$

$$w_1 = \sqrt[4]{\sqrt{2}}.(cos(\tfrac{\pi}{16} + 1.\tfrac{2.\pi}{4}) + isen(\tfrac{\pi}{16} + 1.\tfrac{2.\pi}{4})) =$$

$$= \sqrt[4]{\sqrt{2}}.(cos(\tfrac{9}{16}.\pi) + isen(\tfrac{9}{16}.\pi));$$

$$w_2 = \sqrt[4]{\sqrt{2}}.(cos(\tfrac{\pi}{16} + 2.\tfrac{2.\pi}{4}) + isen(\tfrac{\pi}{16} + 2.\tfrac{2.\pi}{4})) =$$

$$= \sqrt[4]{\sqrt{2}}.(cos(\tfrac{17}{16}.\pi) + isen(\tfrac{17}{16}.\pi)); \text{ y}$$

$$w_3 = \sqrt[4]{\sqrt{2}}.(cos(\tfrac{\pi}{16} + 3.\tfrac{2.\pi}{4}) + isen(\tfrac{\pi}{16} + 3.\tfrac{2.\pi}{4})) =$$

$$= \sqrt[4]{\sqrt{2}}.(cos(\tfrac{25}{16}.\pi) + isen(\tfrac{25}{16}.\pi)).$$



5.3.1. Raíces n-ésimas de la unidad

Dado $n \in \mathbb{N}$, las raíces n-ésimas de la unidad son los números complejos w tales que $w^n = 1$. De acuerdo a lo visto precedentemente se trata de los complejos

$$w_k = cos(k.\frac{2.\pi}{n}) + i\, sen(k.\frac{2.\pi}{n})$$

con k entero, $0 \leq k \leq n-1$.

Llamamos G_n al conjunto de las **raíces n-ésimas de la unidad**, es decir,

$$G_n = \{w_k,\ 0 \leq k \leq n-1\}.$$

Observar que los elementos de G_n se corresponden con los vértices del polígono n-regular inscripto en la circunferencia de radio 1 que contiene al punto $(1,0)$.

Ejemplo 196.

$G_1 = \{1\}$ $\quad$ $G_2 = \{1, -1\}$

$G_3 = \{1, -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{1}{2} - \frac{\sqrt{3}}{2}i\}$ $\quad$ $G_4 = \{1, -1, i, -i\}$

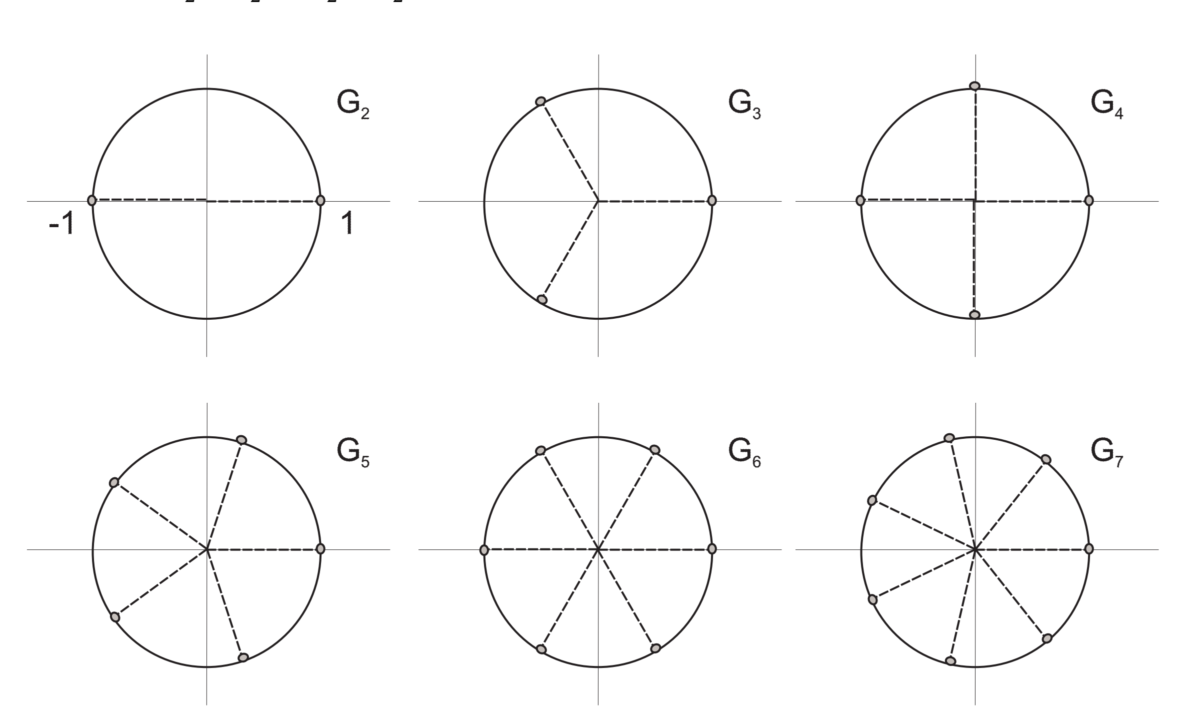


Figura 5.6: representación de las raíces n-ésimas de la unidad.

♢

La operación producto es cerrada en G_n, es decir si z y w son raíces n-ésimas de la unidad, entonces $z.w$ también es raíz n-ésima de la unidad pues $(z.w)^n = z^n.w^n =$

$1.1 = 1$. En forma análoga se prueba que si $z \in G_n$ entonces $z^{-1} \in G_n$ y $\overline{z} \in G_n$. Observar que si $\mid z \mid= 1$ entonces $z^{-1} = \overline{z}$. Además, si $z \in G_n$ entonces $z^{-1} = z^{n-1}$.
Un número complejo w se dice una **raíz primitiva de orden n de la unidad** si $w^n = 1$ y $w^m \neq 1$ para todo natural m tal que $m < n$.
Es claro que si w es una raíz primitiva de orden n de la unidad entonces $w \in G_n$. La recíproca en general no es verdadera, por ejemplo $-1 \in G_4$ pero -1 no es raíz primitiva de orden 4 sino que es raíz primitiva de orden 2. La siguiente proposición nos dice cuales son los elementos de G_n que son raíces primitivas de orden n.

Proposición 197. *Sea $k \in \mathbb{N}$ con $0 \leq k \leq n-1$. El complejo $w_k = cos(k.\frac{2.\pi}{n}) + i\,sen(k.\frac{2.\pi}{n})$ es raíz primitiva de orden n si y sólo si $(k,n) = 1$.*

Demostración: Asumamos que w_k es raíz primitiva de orden n y sea $m = \frac{n}{(n,k)}$. Por De Moivre tenemos que

$$w_k^m = cos(m.k.\tfrac{2.\pi}{n}) + i\,sen(m.k.\tfrac{2.\pi}{n}) = cos(\tfrac{n}{(n,k)}.k.\tfrac{2.\pi}{n}) + i\,sen(\tfrac{n}{(n,k)}.k.\tfrac{2.\pi}{n}) =$$

$$= cos(\tfrac{k}{(n,k)}.2.\pi) + i\,sen(\tfrac{k}{(n,k)}.2.\pi) = cos(0) + i\,sen(0)) = 1.$$

Luego, por definición de raíz primitiva, $m \geq n$, entonces $\frac{n}{(n,k)} \geq n$, de donde $(n,k) = 1$; como queríamos probar.
Ahora asumamos que k es tal que $(n,k) = 1$ y veamos que $w_k = cos(k.\frac{2.\pi}{n}) + i\,sen(k.\frac{2.\pi}{n})$ es una raíz primitiva de orden n.

(a) $w_k^n = cos(n.k.\frac{2.\pi}{n}) + i\,sen(n.k.\frac{2.\pi}{n}) = cos(0) + i\,sen(0) = 1$.

(b) Si $m \in \mathbb{N}$ y $w_k^m = 1$ entonces $cos(m.k.\frac{2.\pi}{n}) + i\,sen(m.k.\frac{2.\pi}{n}) = 1$; luego existe $h \in \mathbb{Z}$ tal que $m.k.\frac{2.\pi}{n} + h.2.\pi = 0$, de donde $m.k = -n.h$.
Como k y n son coprimos tenemos que n divide a m; y como ambos son positivos debe ser $m \geq n$.

De (a) y (b) resulta que w_k es primitiva de orden n. □

Corolario 198. *Si $w \in G_p$, p primo y $w \neq 1$ entonces w es primitiva de orden p.*

Corolario 199. *Si w es raíz primitiva de orden n de la unidad entonces*

$$G_n = \{w, w^2, w^3, ..., w^{n-1}, 1\}.$$

Demostración: Es claro que $\{w, w^2, w^3, ..., w^{n-1}, w^n\} \subset G_n$ pues $(w^m)^n = (w^n)^m = 1^m = 1$ para cualquier m. Ahora supongamos que dos de estas potencias son iguales, es decir, supongamos que existen s y t con $1 \leq s < t \leq n$ tales que $w^t = w^s$. En tal caso $w^{t-s} = 1$; como w es primitiva de orden n y $t-s < n$ debe ser $t-s = 0$. Luego $t = s$ contradiciendo la suposición $s < t$. Resulta que $\{w, w^2, w^3, ..., w^{n-1}, 1\}$ tiene exactamente n elementos; como G_n tiene n elementos debe ser $\{w, w^2, w^3, ..., w^{n-1}, 1\} = G_n$ como queríamos probar. □

Proposición 200. *Sea w una raíz primitiva de orden n de la unidad y $k \in \mathbb{Z}$. Se satisface que*

$$w^k \text{ es raíz primitiva de orden } n \Leftrightarrow (n, k) = 1.$$

Demostración: Asumamos que w^k es primitiva de orden n, veremos que $(n, k) = 1$. Como $(w^k)^{\frac{n}{(n,k)}} = (w^n)^{\frac{k}{(n,k)}} = 1^{\frac{n}{(n,k)}} = 1$ y w^k es primitiva de orden n entonces debe ser $\frac{n}{(n,k)} \geq n$, luego $(n, k) = 1$.
Ahora asumamos $(n, k) = 1$ y veamos que w^k es primitiva de orden n.

(a) $(w^k)^n = (w^n)^k = 1^k = 1$.

(b) Si $m \in \mathbb{N}$ y $(w^k)^m = 1$, entonces $w^{k.m} = 1$. Por el algoritmo de la división existen enteros q y r tales que $k.m = q.n+r$ con $0 \leq r < n$; luego $w^{k.m} = w^{q.n+r} = (w^n)^q.w^r = 1^q.w^r = w^r = 1$; entonces $r = 0$, pues $r < n$ y por hipótesis w es primitiva de orden n. Así tenemos que $k.m = q.n$; como n y k son coprimos resulta que n divide a m, lo cual implica $n \leq m$ pues ambos son positivos.

De (a) y (b) obtenemos que w^k es raíz primitiva de orden n. □

Vimos que todo complejo z_0 admite exactamente n raíces n-ésimas. La siguiente proposición nos muestra cómo a partir de una de estas raíces podemos calcular las restantes conociendo los elementos de G_n.

Proposición 201. *Sea z es una raíz n-ésima cualquiera de z_0. Las raíces n-ésimas de z_0 son $z.w$ con $w \in G_n$.*

Demostración: Ejercicio. □

Ejemplo 202.

Como $(2+i)^4 = -7+24i$, es decir, como $2+i$ es una raíz cuarta de $-7+24i$, y como $G_4 = \{1, i, -1, -i\}$, entonces las raíces cuartas de $-7+24i$ son:

$(2+i).1 = 2+i$;

$(2+i).i = -1+2i$;

$(2+i).(-1) = -2-i$; y

$(2+i).(-i) = 1-2i$.

$\diamondsuit$

Ejercicio 203.

1. La suma de las raíces n-ésimas de un número complejo es igual a cero. $\diamondsuit$

Capítulo 6

Estructuras algebraicas

6.1. Operaciones en un conjunto

Sea A un conjunto no vacío. Una **ley de composición interna** u **operación** en A es una función de $A \times A$ en A; es decir, una aplicación que a cada par ordenado de elementos de A le hace corresponder uno y solo un elemento de A. Si $*$ es una operación en A y x e y son elementos de A, entonces la imagen por $*$ de (x, y) se denotará $x * y$.

Ejemplo 204.

- La suma $+$ es una operación en el conjunto de los números reales: dados dos reales a y b cualesquiera, la operación suma les hace corresponder el numero real que se denota $a + b$.
- El producto . es una operación en el conjunto de los números reales.
- La aplicación $\star$ de $\mathbb{Z} \times \mathbb{Z}$ en $\mathbb{Z}$ que a cada par (n, m) le hace corresponder el entero que se denota $n \star m$ dado por $n \star m = 2.n + 3.m$ (donde $+$ y . son la suma y el producto usual en $\mathbb{Z}$) es una operación en $\mathbb{Z}$. Así, por ejemplo, tenemos que

$$-2 \star 1 = 2.(-2) + 3.1 = -1$$

$$2 \star 3 = 2.2 + 3.3 = 13$$

$$0 \star 10 = 2.0 + 3.10 = 30$$

- La operación $\diamondsuit$ definida en el conjunto de los números naturales en la forma $m \diamondsuit n = m^2 + n$.
- Sea $B^B = \{$ funciones de B en $B\}$, donde B es un conjunto cualquiera. La

composición de funciones $\circ$ es una operación en B^B. Recordar que si f y g son funciones de B en B entonces $g \circ f$ es la función de B en B dada por

$$(g \circ f)(x) = g(f(x)) \text{ para todo } x \text{ en } B.$$

- La unión $\cup$, la intersección $\cap$, la diferencia $-$, la diferencia simétrica $\triangle$ son todas operaciones definidas en el conjunto de partes $\mathcal{P}(E)$, para E un conjunto cualquiera. $\diamondsuit$

Sea $*$ una operación definida en A y sea A' un subconjunto de A. Se dice que $*$ es **cerrada** en A' cuando $x * y \in A'$ para todo par de elementos x e y de A'. En tal caso, cuando $*$ es cerrada en A', resulta que $*$ es también una operación en A' (en rigor, la restricción de $*$ a $A' \times A'$).

Ejemplo 205.

- La suma $+$ de $\mathbb{R}$ es cerrada en $\mathbb{N}$, esto quiere decir que la suma de dos naturales es un natural, por ende la suma es también una operación en $\mathbb{N}$.
- La composición de funciones $\circ$ es cerrada en el subconjunto B' de B^B formado por las funciones de B en B que son biyectivas, es decir: la composición de dos funciones biyectivas es una función biyectiva.

  En particular resulta que $\circ$ es una operación en el conjunto S_n de permutaciones del intervalo natural $\mathbb{I}_n$, es decir, en $S_n = \{f : \mathbb{I}_n \to \mathbb{I}_n \text{biyectiva}\}$.
- La operación $\star$ definida en $\mathbb{Z}$ en la forma $n \star m = n - 3.m$ no es cerrada en $\mathbb{N}$, pues, por ejemplo, $1 \in \mathbb{N}$ y $2 \in \mathbb{N}$ pero $1 \star 2 = 1 - 3.2 = -5 \notin \mathbb{N}$. $\diamondsuit$

Sea $*$ una operación definida en A. Se dice que $*$ es **asociativa** si

$$x * (y * z) = (x * y) * z \text{ para todo } x,\ y,\ z \text{ en } A.$$

Se dice que $*$ es **conmutativa** si

$$x * y = y * x \text{ para todo } x,\ y \text{ en } A.$$

Se dice que $*$ **admite elemento neutro** si

existe $e \in A$ tal que $x * e = e * x = x$ para todo x en A.

En tal caso e se llama **elemento neutro** de $*$.

Se dice que un elemento x de A **admite opuesto** según $*$ si

existe un elemento $x' \in A$ tal que $x * x' = x' * x = e$

donde e es el elemento neutro de $*$. El elemento x' se llama **opuesto** de x según la operación $*$.

Observar que si $*$ no admite neutro entonces ningún elemento tiene opuesto según $*$.

Ejemplo 206.

- Hemos visto en los capítulos anteriores que la operación $+$ en $\mathbb{R}$ es asociativa, conmutativa, admite neutro que es el 0 y cada real x tiene por opuesto según la suma al real que se denota $-x$.
- La operación producto . en $\mathbb{R}$ es asociativa, conmutativa, admite neutro que es el 1 y cada elemento $x \neq 0$ tiene por opuesto según el producto al real que se denota x^{-1}. Para diferenciar el opuesto según la suma del opuesto según el producto se dice simplemente opuesto cuando se trata del opuesto según la suma $-x$ y se dice **inverso** cuando se trata del opuesto según el producto x^{-1}. Observar que 0 no admite inverso pues para todo $x \in \mathbb{R}$ se cumple que $x.0 = 0 \neq 1$.
- Sea $\star$ la operación definida en $\mathbb{Z}$ en la forma $n \star m = n - 3.m$. Como

  $$(n \star m) \star r = (n - 3.m) \star r = (n - 3.m) - 3.r = n - 3.m - 3.r$$
  $$n \star (m \star r) = n \star (m - 3.r) = n - 3.(m - 3.r) = n - 3.m - 9.r$$

  la operación $\star$ no es asociativa.
  Por ejemplo, $(1 \star 2) \star 3 = -14 \neq -32 = 1 \star (2 \star 3)$.
  Análogamente se ve que $\star$ no es conmutativa.
  Si $\star$ admite un neutro e entonces debe cumplirse $n \star e = e \star n$ para todo $n \in \mathbb{Z}$; luego, para todo $n \in \mathbb{Z}$ debe cumplirse que $n - 3.e = e - 3.n$; de donde, para todo $n \in \mathbb{Z}$ se tiene que satisfacer que $4.e = 4.n$; es decir, $e = n$ para todo entero n. Claramente, la operación $\star$ no admite neutro.
- Sea $E = \mathcal{P}(U)$ el conjunto de partes de un universal. La unión $\cup$ y la intersección $\cap$ son operaciones en E con las siguientes propiedades:
  - $\cup$ y $\cap$ son asociativas.
  - $\cup$ y $\cap$ son conmutativas.
  - $\cup$ tiene elemento neutro: el conjunto vacío $\emptyset$.
  - $\cap$ tiene elemento neutro: el conjunto universal U.

- Veamos si un conjunto S admite opuesto S' según la unión. En tal caso, debe ser $S \cup S' = \emptyset$; luego $S = S' = \emptyset$. Resulta que el único conjunto que admite opuesto según la unión es el vacío y su opuesto es el mismo conjunto vacío.
- Veamos si un conjunto S admite opuesto S' según la intersección. En tal caso, debe ser $S \cap S' = U$; luego $S = S' = U$. Resulta que el único conjunto que admite opuesto según la intersección es el conjunto universal y su opuesto es el mismo conjunto universal. ♢

Convención: Para tener similitud con lo convenido en el caso de los números reales, cuando una operación se simboliza **aditivamente** (con el símbolo $+$), el neutro se denota 0 y el opuesto de un elemento x se escribe $-x$.
Cuando la operación se simbliza **multiplicativamente** (con el símbolo .), el neutro se denota 1 y el opuesto de un elemento x se escribe x^{-1} y se dice inverso.

Proposición 207. *Sea $*$ una operación asociativa con neutro e en un conjunto A y sean $a, b \in A$.*

1. *Si x es neutro de $*$ entonces $e = x$ (unicidad del neutro).*
2. *Si a' y x son opuestos de a (según $*$) entonces $a' = x$ (unicidad de opuestos).*
3. *Si b' es el opuesto de b y a' es el opuesto de a, entonces $b' * a'$ es el opuesto de $a * b$.*
4. *Si a' es el opuesto de a entonces el opuesto de a' es a.*

Demostración: 1. $e = e * x$ porque x es neutro, y $e * x = x$ porque e es nuetro; resulta $e = x$.
2. $a' = a' * e = a' * (a * x) = (a' * a) * x = e * x = x$ porque e es nuetro, porque $a * x = x * a = a * a' = a' * a = e$ y porque $*$ es asociativa.
3. $(a*b)*(b'*a') = ((a*b)*b')*a' = (a*(b*b'))*a' = (a*e)*a' = a*(e*a') = a*a' = e$.
Análogamente tenemos que $(b' * a') * (a * b) = e$; luego $b' * a'$ es el opuesto de $a * b$, como queríamos probar.
4. Se deja como ejercicio. □

Sea A un conjunto en el cual están definidas dos operaciones $+$ y . .
Se dice que . es **distributiva a izquierda** con respecto a $+$ si

$x.(y + z) = x.y + x.z$ cualesquiera sean x, y, z en A;

y se dice que . es **distributiva a derecha** con respecto a + si

$(y+z).x = y.x + z.x$ cualesquiera sean x, y, z en A.

Si la operación es distributiva a izquierda y a derecha entonces se dice **distributiva**.

Ejemplo 208.

- El producto . es distributivo con respecto a la suma + en $\mathbb{R}$.
- La unión $\cup$ es distributiva con respecto a la intersección $\cap$ en $\mathcal{P}(U)$.
- La intersección $\cap$ es distributiva con respecto a unión $\cup$ en $\mathcal{P}(U)$.

6.1.1. Suma y producto en $\mathbb{Z}_n$

Como vimos en el Capítulo 4, si n es un natural, $\mathbb{Z}_n$ es el conjunto cociente de $\mathbb{Z}$ por la relación de equivalencia $\equiv mod(n)$. Es decir,

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\},$$

donde $\overline{k} = \{m \in \mathbb{Z} : m \equiv k \, mod(n)\} = \{m \in \mathbb{Z} : r_n(m) = r_n(k)\}$.

Definiremos en $\mathbb{Z}_n$ una operación suma y una operación producto. Momentaneamente, para diferenciarlas de las operaciones suma de enteros que denotamos + y producto de enteros que denotamos ., las denotaremos $\oplus$ y $\odot$. Luego solo escribiremos + y . entendiendo que del contexto surgirá si nos referimos a una operación entre enteros (elementos de $\mathbb{Z}$) o a una operación entre enteros módulo n (elementos de $\mathbb{Z}_n$).

Para $\overline{a}$ y $\overline{b}$ cualesquiera en $\mathbb{Z}_n$ se define:

$$\overline{a} \oplus \overline{b} = \overline{a+b} \qquad \text{y} \qquad \overline{a} \odot \overline{b} = \overline{a.b}.$$

Ejemplo 209.

- En $\mathbb{Z}_5$
  $\overline{2} \oplus \overline{2} = \overline{2+2} = \overline{4}$; $\quad \overline{2} \odot \overline{2} = \overline{2.2} = \overline{4}$;
  $\overline{2} \oplus \overline{3} = \overline{2+3} = \overline{5} = \overline{0}$; $\quad \overline{2} \odot \overline{3} = \overline{2.3} = \overline{6} = \overline{1}$
  $\overline{2} \oplus \overline{4} = \overline{2+4} = \overline{6} = \overline{1}$; $\quad \overline{2} \odot \overline{4} = \overline{2.4} = \overline{8} = \overline{3}$.
- En $\mathbb{Z}_4$
  $\overline{2} \oplus \overline{2} = \overline{2+2} = \overline{0}$; $\quad \overline{2} \odot \overline{2} = \overline{2.2} = \overline{4} = \overline{0}$;
  $\overline{2} \oplus \overline{3} = \overline{2+3} = \overline{5} = \overline{1}$; $\quad \overline{2} \odot \overline{3} = \overline{2.3} = \overline{6} = \overline{2}$
  $\overline{2} \oplus \overline{4} = \overline{2+4} = \overline{6} = \overline{2}$; $\quad \overline{2} \odot \overline{4} = \overline{2.4} = \overline{8} = \overline{0}$.

Proposición 210. *La suma $\oplus$ y el procuto $\odot$ definidos en $\mathbb{Z}_n$ son operaciones asociativas, conmutativas y admiten elemento neutro. El neutro para $\oplus$ es $\overline{0}$ y el neutro para $\odot$ es $\overline{1}$. Todo elemento tiene opuesto según $\oplus$.*

Demostración: Sean $\overline{a}$, $\overline{b}$ y $\overline{c}$ elementos cualesquiera de $\mathbb{Z}_n$.

$$(\overline{a} \oplus \overline{b}) \oplus \overline{c} = \overline{a+b} \oplus \overline{c} = \overline{(a+b)+c}.$$

$$\overline{a} \oplus (\overline{b} \oplus \overline{c}) = \overline{a} \oplus \overline{b+c} = \overline{a+(b+c)}.$$

Como la suma de enteros $+$ es asociativa, tenemos que $(a+b)+c = a+(b+c)$; luego

$(\overline{a} \oplus \overline{b}) \oplus \overline{c} = \overline{a} \oplus (\overline{b} \oplus \overline{c})$; como queríamos probar.

Las restantes demostraciones son análogas y se dejan como ejercicios. □

Proposición 211. *Un elemento $\overline{a} \in \mathbb{Z}_n$ admite opuesto según $\odot$ si y sólo si a y n son coprimos.*

Demostración: Para probar la implicación directar, observar que

$\overline{b}$ es opuesto de $\overline{a}$ según $\odot \to \overline{a} \odot \overline{b} = \overline{1} \to \overline{a.b} = \overline{1} \to a.b \equiv 1\, mod(n) \to$

$\to n$ divide a $a.b - 1 \to$ existe $k \in \mathbb{Z}$ tal que $a.b - 1 = k.n \to$

$\to$ existe $k \in \mathbb{Z}$ tal que $1 = a.b - k.n \to (a, n) = 1$.

La recíproca se prueba en forma análoga. □

Ejemplo 212.

En la siguiente tabla está representada la operación producto en $\mathbb{Z}_6$.

$\odot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Observar que los únicos elementos que admiten inverso son $\overline{1}$ (el inverso es el mismo $\overline{1}$) y $\overline{5}$ (el inverso es el mismo $\overline{5}$). Es fácil ver en la tabla que ninguno de los restantes elementos puede ser multiplicado para obtener $\overline{1}$ como resultado.
La simetría de la tabla respecto de la diagonal indica que la operación es conmutativa.
Observar que no vale la propiedad cancelativa respecto del producto, por ejemplo:

$$\overline{2} \odot \overline{2} = \overline{2} \odot \overline{5}$$

sin embargo $\overline{2} \neq \overline{5}$. ♢
En adelante escribiremos $+$ en lugar de $\oplus$ y . en lugar de $\odot$. Estas operaciones se llaman respectivamente **suma y producto de enteros módulo n**.

6.2. Grupo. Anillo. Cuerpo

Sea G un conjunto y $*$ una operación en G. El par $(G, *)$ se dice

- un **semigrupo** si $*$ es asociativa;
- un **grupo** si $*$ es asociativa, admite elemento neutro, y todo elemento de G admite opuesto según $*$;
- un **grupo conmutativo** o **grupo abeliano** si es grupo y $*$ es conmutativa.

Ejemplo 213.

- $(\mathbb{C}, +)$ es un grupo conmutativo.
- $(\mathbb{C}, .)$ no es un grupo porque el elemento 0 no admite inverso.
- $(\mathbb{R}, +)$; $(\mathbb{Q}, +)$ y $(\mathbb{Z}, +)$ son grupos conmutativos.
- $(\mathbb{N}, +)$ es un semigrupo, pero no es un grupo: la suma no tiene neutro en $\mathbb{N}$. (Recordar que convinimos que $0 \notin \mathbb{N}$).
- $(S_n, \circ)$ es un grupo no conmutativo. S_n es el conjunto de las permutaciones de n elementos (funciones biyectivas de $\mathbb{I}_n$ en I_n) y $\circ$ es la composición de funciones.
- $(G_n, .)$ es un grupo conmutativo. G_n es el conjunto de las raíces n-ésimas de la unidad y . es el producto usual de complejos.
- $(\mathbb{Z}_n, +)$ es un grupo conmutativo. 

Proposición 214. *En todo grupo $(G, *)$ vale la propiedad cancelativa respecto de $*$, es decir, para todo $a, b, c \in G$,*

$$a * b = a * c \text{ implica } b = c.$$

Demostración: Operar a ambos lados de la igualdad con c', el opuesto de c. □

Ejercicio 215.

1. Determinar si $(\mathbb{R}^+, *)$ es grupo, donde $*$ es la operación $x * y = 2.x.y$.
2. Probar que si $(G, +)$ y $(H, .)$ son grupos, entonces $(G \times H, \otimes)$ es un grupo, donde $G \times H$ es el producto cartesiano de G y H, y $\otimes$ es la operación definida en $G \times H$ en la forma

   $$(g_1, h_1) \otimes (g_2, h_2) = (g_1 + g_2, h_1.h_2).$$

   La operación $\otimes$ así definida se llama operación producto de las operaciones $+$ y $.$; y $(G \times H, \otimes)$ se llama **grupo producto** de $(G, +)$ y $(H, .)$.
   Determinar el elemento neutro de $\otimes$ y los opuestos. ♢

Ejemplo 216.
Si definimos en $\mathbb{Z} \times \mathbb{R}^+$ la operación $*$ en la forma

$$(m, x) * (n, y) = (m + n, x.y)$$

resulta que $(\mathbb{Z} \times \mathbb{R}^+, *)$ es un grupo. El neutro es $(0, 1)$, y el opuesto de un (a, b) cualquiera es $(-a, \frac{1}{b})$. ♢

Sea A un conjunto en el cual están definidas dos operaciones $+$ y $.$. La terna $(A, +, .)$ se dice

- un **anillo** si $(A, +)$ es un grupo conmutativo, $(A, .)$ es un semigrupo y $.$ es distributiva respecto de $+$.
- un **anillo conmutativo** o **anillo abeliano** si es anillo y $.$ es conmutativa.
- un **anillo con unidad** si es anillo y $.$ admite elemento neutro.
- un **anillo de integridad** si es anillo y para todo $x, y \in A$ se verifica que

$$\text{si } x.y = 0 \text{ entonces } x = 0 \text{ o } y = 0.$$

Ejemplo 217.

- $(\mathbb{C}, +, .)$, $(\mathbb{R}, +, .)$, $(\mathbb{Q}, +, .)$, $(\mathbb{Z}, +, .)$ son todos anillos conmutativos con unidad y de integridad. Las operaciones + y . son la suma y el producto usual.
- $(\mathbb{Z}_n, +, .)$ es un anillo conmutativo con unidad. Es de integridad si y solo si n es primo. Las operaciones + y . son la suma y el producto módulo n que fueron definidas en la Sección 6.1.1.
  Observar que, por ejemplo, en $\mathbb{Z}_8$ se tiene que $\overline{2}.\overline{4} = \overline{0}$, pero $\overline{2} \neq \overline{0}$ y $\overline{4} \neq \overline{0}$.

Ejercicio 218. Determinar si $(\mathcal{P}(U), \triangle, \cap)$ es un anillo, donde U es un conjunto cualquiera. ♢

Proposición 219. *Sea $(A, +, .)$ un anillo y sean $a, b, c \in A$.*

1. $a\,.\,0 = 0.a = 0$.
2. $(-a).b = a.(-b) = -(a.b)$.
3. $(-a).(-b) = a.b$.
4. *Si A es anillo de integridad y $a \neq 0$ entonces*

$$a.b = a.c \text{ implica } b = c.$$

Demostración: 1. $a = a + 0$ pues 0 es neutro de +. Multiplicando ambos miembros por a y en virtud de la propiedad distributiva, tenemos $a.a = a.a + a.0$. Sumando el opuesto de $a.a$ a ambos miembros resulta

$$0 = -(a.a) + a.a = -(a.a) + (a.a + a.0) = (-(a.a) + (a.a)) + a.0 = 0 + a.0 = a.0;$$

luego $0 = a.0$ como queríamos probar.
2. Como $a.b + (-a).b = (a + (-a)).b = 0.b = 0$, tenemos que $a.b + (-a).b = 0$. Sumando $-(a + b)$ a ambos miembros resulta que $(-a).b = -(a + b)$.
Las restantes demostraciones son similares y quedan como ejercicios. □

Sea K un conjunto en el cual están definidas dos operaciones + y .. La terna $(K, +, .)$ es un **cuerpo** si $(K, +, .)$ es un anillo con unidad tal que todo elemento no nulo de K (distinto del elemento neutro de +) tiene inverso (opuesto según .).
Si además la operación . es conmutativa entonces $(K, +, .)$ se dice **cuerpo conmutativo o abeliano**.

Ejemplo 220.

- $(\mathbb{C}, +, .)$, $(\mathbb{R}, +, .)$, $(\mathbb{Q}, +, .)$ son cuerpos conmutativos.
- $(\mathbb{Z}, +, .)$ no es un cuerpo: existen elementos no nulos de $\mathbb{Z}$ que no admiten inverso. De hecho los únicos elementos de $\mathbb{Z}$ que admiten inverso en $\mathbb{Z}$ son 1 y -1.
- Para todo p primo, $(\mathbb{Z}_p, +, .)$ es un cuerpo.

Proposición 221. *Si $(K, +, .)$ es un cuerpo entonces $(K, +, .)$ es un anillo de integridad.*

Demostración: Sean x e y elementos de K tales que $x.y = 0$. Si $x \neq 0$, como $(K, +, .)$ es un cuerpo, x admite inverso x^{-1}, luego

$$y = 1.y = (x^{-1}.x).y = x^{-1}.(x.y) = x^{-1}.0 = 0.$$

□

Un grupo, un anillo, o un cuerpo se dice **finito** si el conjunto sobre el que está definido es finito, en este caso el cardinal del conjunto se dice el **orden** del grupo, anillo o cuerpo, respectivamente.

Ejercicio 222.
Determinar si $\mathbb{Z}_3 \times \mathbb{Z}_3$ con las operaciones + y . es un cuerpo. Dichas operaciones se definen en la forma

$$(a, b) + (a', b') = (a + a', b + b') \text{ y } (a, b).(a', b') = (a.a', b.b').$$

♢

6.2.1. Subgrupo. Subanillo. Subcuerpo

Sea $(G, *)$ un grupo y sea $H \subset G$. Si $*$ es cerrada en H entonces $*$ es una operación en H (en rigor, la restricción de $*$ a H). Cuando $(H, *)$ es un grupo se dice que $(H, *)$ es un **subgrupo** de $(G, *)$.
También puede decirse que H es un subgrupo de $(G, *)$ quedando sobreentendido que es con la operación inducida en H por $*$.

Ejemplo 223.

- $(\mathbb{R}, +)$ es un subgrupo de $(\mathbb{C}, +)$.

- $(\mathbb{Q},+)$ es un subgrupo de $(\mathbb{R},+)$.
- $(\mathbb{Q},+)$ es un subgrupo de $(\mathbb{C},+)$.
- Si H es el subconjunto $\{\overline{0},\overline{2},\overline{4},\overline{6}\}$ de $\mathbb{Z}_8$, entonces $(H,+)$ es subgrupo de $(\mathbb{Z}_8,+)$. $\diamondsuit$

Ejercicio 224.

Probar que si $(T,*)$ es subgrupo de $(H,*)$ y $(H,*)$ es subgrupo de $(G,*)$ entonces $(T,*)$ es subgrupo de $(G,*)$.

Proposición 225. *Sea $(G,*)$ un grupo y sea H un subconjunto no vacío de G. Si para todo par de elementos x e y de H se verifica que $x*y' \in H$ (donde y' es el opuesto de y según $*$) entonces $(H,*)$ es un subgrupo de $(G,*)$.*

Demostración: Para probar que $(H,*)$ es grupo basta probar que $*$ es cerrada en H, que el neutro e de $*$ en G pertenece a H, y que el opuesto de cada elemento de H es también un elemento de H.
Por hipótesis sabemos que

$$(x \in H \wedge y \in H) \to x*y' \in H. \tag{6.1}$$

Como H es no vacío existe $a \in H$; entonces por (6.1) tenemos que $a*a' = e \in H$.
Sea x un elemento cualquiera de H. Como $e \in H$ y $x \in H$, por (6.1) tenemos que $e*x' = x' \in H$.
Finalmente, sean $x, y \in H$ cualesquiera. Por lo anterior $y' \in H$, luego $x \in H$ e $y' \in H$, entonces por (6.1) tenemos que $x*(y')' = x*y \in H$. $\square$
Una forma equivalente de la proposición anterior escrita con notación aditiva es la siguiente. Sea $H \subset G$; vale que

$$H \text{ es un subgrupo de } (G,+) \leftrightarrow \begin{cases} 0 \in H; \\ (x \in H \wedge y \in H) \to x+(-y) \in H; \end{cases}$$

Y en notación multiplicativa es: Sea $H \subset G$; vale que

$$H \text{ es un subgrupo de } (G,.) \leftrightarrow \begin{cases} 1 \in H; \\ (x \in H \wedge y \in H) \to x.y^{-1} \in H; \end{cases}$$

Ejemplo 226.

Sea $H = \{n + m.\sqrt{2} \text{ con } n, m \in \mathbb{Z}\} \subset \mathbb{R}$. Veremos que H es un subgrupo de $(\mathbb{R},+)$:
H es no vacío pues $0 = 0 + 0.\sqrt{2} \in H$.

Sean $x = n + m.\sqrt{2}$ e $y = r + s.\sqrt{2}$ con $n, m, r, s \in \mathbb{Z}$ elementos cualesquiera de H. Como $x+(-y) = (n+m.\sqrt{2})-(r+s.\sqrt{2}) = (n-r)+(m-s).\sqrt{2}$ y $n-r, m-s \in \mathbb{Z}$, resulta que $x + (-y) \in H$.

Concluimos usando la proposición anterior que $(H, +)$ es subgrupo de $(\mathbb{R}, +)$. ♢

Ejercicio 227.

1. Probar que cualquier grupo $(G, *)$ tiene al menos los siguientes subgrupos: $(G, *)$ y $(\{e\}, *)$, donde e es el neutro de $*$.
2. Si H_1 y H_2 son subgrupos de G entonces $H_1 \cap H_2$ es un subgrupo de G.
3. Si $(H_i)_{i\in I}$ es una familia de subgrupos de G entonces $H = \bigcap_{i\in I} H_i$ es un subgrupo de G. ♢

Sea $(G, *)$ un grupo con nuetro e. Para $a \in G$ y $m \in \mathbb{Z}$, se define:

$$a^m = \begin{cases} e, & \text{si } m = 0; \\ a^{m-1} * a, & \text{si } m \geq 1; \\ (a')^{-m}, & \text{si } m < 0; \text{ (donde } a' \text{ es el opuesto de } a \text{ según } *). \end{cases}$$

Cuando el grupo está notado aditivamente en lugar de escribir a^m escribiremos $m \cdot a$.

Ejercicio 228.

1. Sea $(G, *)$ un grupo. Probar que para a y b elementos cualesquiera de G y enteros n y m se satisface que

   i.) $a^{n+m} = a^n * a^m$.

   ii.) $(a^n)^m = a^{n.m}$.

   iv.) $(a')^n = a^{-n} = (a^n)'$, donde $'$ indica opuesto según $*$.

   Además, si $*$ es conmutativa entonces $(a * b)^n = a^n * b^n$.
2. Escribir el enunciado del ejercicio anterior en notación aditiva y multiplicativa; es decir, cuando se trata de un grupo $(G, +)$ o de un grupo $(G, .)$, respectivamente. ♢

Sea $(G, *)$ un grupo y S un subconjunto cualquiera de G. La intersección de todos los subgrupos $(H, *)$ de G que contienen a S se llama **subgrupo generado** por S y se denota $< S >$; es el menor subgrupo de G que contiene a S. Cuando S tiene un único elemento x en lugar de $< \{x\} >$ escribiremos $< x >$.

Proposición 229. *Si* $(G, .)$ *es un grupo y* $g \in G$ *entonces*

$$< g >= \{g^m \ con \ \ m \in \mathbb{Z}\}.$$

(Notación aditiva) Si $(G, +)$ *es un grupo y* $g \in G$ *entonces*

$$< g >= \{m \cdot g \ con \ \ m \in \mathbb{Z}\}.$$

Demostración: Llamemos H a $\{g^m$ con $m \in \mathbb{Z}\}$. Para probar que H es el subgrupo generado por G debemos probar que $g \in H$, que H es grupo y que H está contenido en todo subgrupo de $(G, .)$ que contenga a g.
Como $g = g^1$ tenemos que $g \in H$.
Si x e y son elementos cualesquiera de H, entonces existen enteros n y m tales que $x = g^n$ e $y = g^m$; luego, por las propiedades vistas en ejercicio anterior, tenemos que

$$x.y^{-1} = g^n.(g^m)^{-1} = g^n.g^{-m} = g^{n-m};$$

como $n - m \in \mathbb{Z}$ resulta $x.y^{-1} \in H$; de donde, por la Proposición 225, $(H, .)$ es subgrupo de $(G, .)$.
Finalmente, sea T un subgrupo de $(G, .)$ tal que $g \in T$; es claro que como $(T, .)$ es grupo y $g \in T$ entonces $g^m \in T$, para todo $m \in \mathbb{Z}$; luego, $H \subset T$. □

Ejemplo 230.

- El subgrupo de $(G_8, .)$ generado por i es $< i >= \{i^m$ con $m \in \mathbb{Z}\} = \{i, -1, -i, 1\}$.
- El subgrupo de $(\mathbb{Z}, +)$ generado por 4 es $< 4 >= \{m \cdot 4$ con $m \in \mathbb{Z}\} = 4.\mathbb{Z}$.
- El subgrupo de $(\mathbb{Z}_{10}, +)$ generado por $\overline{4}$ es $< \overline{4} >= \{m \cdot \overline{4}$ con $m \in \mathbb{Z}\} = \{\overline{4}, \overline{8}, \overline{2}, \overline{6}, \overline{0}\}$.

Ejercicio 231.
Probar que si $S \subset S'$ entonces $< S >$ es subgrupo de $< S' >$. ♢

Proposición 232. *Si* $(S, +)$ *es subgrupo de* $(\mathbb{Z}, +)$ *entonces existe* $k \in \mathbb{Z}$ *tal que* $S =< k >= k.\mathbb{Z}$.

Demostración: Si $S = \{0\}$ la proposición vale pues $\{0\} =< 0 >= 0.\mathbb{Z}$.
Si $S \neq \{0\}$ entonces $\{x \in S \wedge x \geq 1\}$ es un subconjunto no vacío de $\mathbb{N}$. Sea k su primer elemento. Veamos que $S =< k >= \{k.m$ con $m \in \mathbb{Z}\} = k.\mathbb{Z}$.

Como S es subgrupo y $k \in S$ entonces $< k > \subset S$ (ver ejercicio anterior).

Ahora, sea $a \in S$ cualquiera; por el algoritmo de la división existen $q, r \in \mathbb{Z}$ con $0 \leq r < k$ tal que $a = q.k + r$. Si $r \neq 0$ entonces, por ser estricatamente menor que k, tenemos que $r \notin \{x \in S \wedge x \geq 1\}$. Pero $r \in S$, pues $a \in S$, $q.k \in S$ y $r = a - q.k$; luego debe ser $r < 1$ lo cual contradice $r \neq 0$. Resulta $r = 0$, de donde $a = q.k \in < k >$ como queríamos probar. □

Ejercicio 233.

1. Un grupo que puede ser generado por un solo elemento se llama **grupo cíclico**. La proposición anterior muestra que todo subgrupo de $(\mathbb{Z}, +)$ es cíclico. Probar que todo subgrupo de $(\mathbb{Z}_n, +)$ es cíclico. ¿Vale lo mismo para todo subgrupo de $(G_n, .)$?
2. Probar que si $a, b \in \mathbb{Z}$ entonces $< \{a, b\} >=< (a, b) >= \{m \cdot (a, b) \text{ con } m \in \mathbb{Z}\}$, donde (a, b) es el máximo común divisor. Por ejemplo, el sugrupo de $(\mathbb{Z}, +)$ generado por $\{4, 6\}$ es
$$< \{4, 6\} >=< 2 >= \{m \cdot 2 \text{ con } m \in \mathbb{Z}\}.$$
3. Probar que todo grupo cíclico es conmutativo.
4. Probar que el grupo simétrico $(S_n, \circ)$ no es cíclico. ♢

Sea $(A, +, .)$ un anillo y sea $A' \subset A$ tal que $+$ y $.$ son cerradas en A'. Si $(A', +, .)$ es un anillo entonces se dice que $(A', +, .)$ es un **subanillo** de $(A, +, .)$. Si $(A', +, .)$ es anillo conmutativo, con unidad o de integridad, se dice que $(A', +, .)$ es subanillo conmutativo, con unidad o de integridad respectivamente.

Como en el caso de subgrupo puede decirse simplemente que A' es subanillo de $(A, +, .)$, quedando las operaciones sobreentendidas.

Ejemplo 234.

- $(\mathbb{R}, +, .)$ es un subanillo conmutativo con unidad de integridad de $(\mathbb{C}, +, .)$.
- $(\mathbb{Q}, +, .)$ es un subanillo conmutativo con unidad de integridad de $(\mathbb{R}, +, .)$.
- $(\mathbb{Q}, +, .)$ es un subanillo conmutativo con unidad de integridad de $(\mathbb{C}, +, .)$.
- Si H es el subconjunto $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$ de $\mathbb{Z}_8$, entonces $(H, +, .)$ es un subanillo conmutativo (sin unidad) de $(\mathbb{Z}_8, +, .)$. ♢

Proposición 235. *Sea $(A, +, .)$ un anillo y $A' \subset A$.*

$$A' \text{ es subanillo de } (A,+,.) \leftrightarrow \begin{cases} 0 \in A'; \\ (x \in A' \wedge y \in A') \rightarrow (x+y \in A' \wedge x.y \in A'); \\ x \in A' \rightarrow -x \in A'. \end{cases}$$

Si $(A,+,.)$ es anillo con unidad, A' es subanillo con unidad de $(A,+,.)$ si y solo sí A' es subanillo de $(A,+,.)$ y $1 \in A'$.

Demostración: Se deja como ejercicio. □

Ejercicio 236.

1. Si $(A',+,.)$ es subanillo de $(A,+,.)$ entonces $(A',+)$ es un subgrupo conmutativo de $(A,+)$.
2. Si $k \in \mathbb{Z}$ llamamos $k.\mathbb{Z} = \{k.m \text{ con } m \in \mathbb{Z}\}$ al conjunto de los múltiplos enteros de k. Probar que los únicos subanillos de $(\mathbb{Z},+,.)$ son $(k.\mathbb{Z},+,.)$. Observar que estos subanillos son sin unidad a menos que $k=1$, luego el único subanillo con unidad de $\mathbb{Z}$ es el mismo $\mathbb{Z}$. ♢

Sea $(K,+,.)$ un cuerpo y sea $K' \subset K$ tal que $+$ y $.$ son cerradas en K'. Si $(K',+,.)$ es un cuerpo entonces se dice que $(K',+,.)$ es un **subcuerpo** de $(K,+,.)$. Si $(K',+,.)$ es cuerpo conmutativo se dice que $(K',+,.)$ es subcuerpo conmutativo de $(K,+,.)$. Como en el caso de sugrupo y en el caso de subanillo se puede obviar nombrar a las operaciones si las mismas surgen del contexto.

Ejemplo 237.

- $(\mathbb{R},+,.)$ es un subcuerpo conmutativo de $(\mathbb{C},+,.)$.
- $(\mathbb{Q},+,.)$ es un subcuerpo conmutativo de $(\mathbb{R},+,.)$.
- $(\mathbb{Z},+,.)$ no es un subcuerpo de $(\mathbb{R},+,.)$. ♢

Proposición 238. *Sea $(K,+,.)$ un cuerpo y $K' \subset K$.*

$$K' \text{ es subcuerpo de } (K,+,.) \leftrightarrow \begin{cases} 0 \in K' \wedge 1 \in K'; \\ (x \in K' \wedge y \in K') \rightarrow (x+y \in K' \wedge x.y \in K'); \\ x \in K' \rightarrow (-x \in K' \wedge x^{-1} \in K'). \end{cases}$$

Demostración: Se deja como ejercicio. □

Ejemplo 239.

- $\mathbb{Q}$ con la suma y el producto usual es un subcuerpo de $\mathbb{R}$ y éste, a su vez, es un subcuerpo de $\mathbb{C}$.
- $Q[\sqrt{2}] = \{a + b.\sqrt{2}$ con $a, b \in \mathbb{Q}\}$ es un subcuerpo de $\mathbb{R}$.

Capítulo 7

Polinomios

7.1. Suma y producto de polinomios. Propiedades

Sea $(\mathbb{A}, +, .)$ un anillo conmutativo. Llamamos **polinomio en una indeterminada** x **con coeficientes en** $\mathbb{A}$ a toda expresión de la forma;

$$p = \sum_{i=0}^{n} p_i x^i = p_0 x^0 + p_1 x^1 + ... + p_n x^n$$

donde n es un elemento cualquiera de $\mathbb{N}_0$ y $p_i \in \mathbb{A}$ para todo i.

Convenimos que:

$p_i x^i$ se llama **término de grado** i de p. Cuando $i = 0$, en lugar de escribir $p_0 x^0$ podemos escribir simplemente p_0. El término de grado 0 también se dice **término independiente**. Cuando $i = 1$, en lugar de $p_1 x^1$ podemos escribir simplemente $p_1 x$.

p_i se llama **coeficiente del término de grado** i de p. Cuando $p_i = 0$ se dice que el término de grado i es nulo y puede no escribirse. Cuando $p_i = 1$ en lugar de $1x^i$ podemos escribir simplemente x^i.

Si todos los coeficientes son nulos, es decir, si $p_i = 0$ para todo i entonces p se dice el **polinomio nulo** y se escribe $p = 0$.

Si p no es el polinomio nulo, se define el **grado de** p como el mayor i tal que $p_i \neq 0$. Se indica $gr(p)$. Observar que el polinomio nulo no tiene grado.

Si n es el grado de p, $p_n x^n$ se llama el **término principal** de p y p_n se llama el **coeficiente principal**. Observar que el coeficiente principal nunca es nulo.

Si el coeficiente principal es igual a 1 el polinomio se dice **mónico**.

El **conjunto de todos los polinomios** en una indeterminada x con coeficientes en $\mathbb{A}$ se indica $\mathbb{A}[x]$.

Los polinomios se llamarán con letras minúsuculas p, q, h,... Si q es un polinomio entonces, para todo $i \in \mathbb{N}_0$, q_i indica el coeficiente del término de grado i de q.

Ejemplo 240.

En $\mathbb{Z}[x]$ tenemos que $3x^0+0x^1+25x^2+0x^4 = 3x^0+0x+25x^2 = 3x^0+25x^2 = 3+25x^2$ es un polinomio de grado 3; el término principal es $25x^2$ y el coeficiente principal es 25; no es un polinomio mónico; el término de grado 1 es $0x^1$, el coeficiente del término de grado 1 es 0, por eso podemos no escribir este término.

El polinomio $q = \sum_{i=0}^{5} ix^i$ es el polinomio $x + 2x^2 + 3x^3 + 4x^4 + 5x^5$. Observar que para todo $i \leq 5$ se tiene que $q_i = i$ en tanto que para todo $i \geq 6$ se tiene que $q_i = 0$.$\diamondsuit$

Es claro que si un polinomio tiene grado n entonces todos sus términos de grado mayor que n son nulos. Dos polinomios p y q son **iguales** si, para todo i, el coeficiente del término de grado i de p es igual al coeficiente del término de grado i de q; es decir, p y q son iguales si para todo i se verifica que $p_i = q_i$. En particular, si dos polinomios son iguales y no nulos entonces tienen igual grado.

En $\mathbb{A}[x]$ definimos dos operaciones, suma de polinomios que se indica $+$ y producto de polinomios que se indica . , de la siguiente manera: si p y q son polinomios cualesquiera de $\mathbb{A}[x]$ entonces

$p + q$ es el polinomio de $\mathbb{A}[x]$ tal que $(p + q)_i = p_i + q_i$ para todo i;

$p.q$ es el polinomio de $\mathbb{A}[x]$ tal que $(p.q)_i = \sum_{j=0}^{i}(p_j.q_{i-j})$ para todo i.

Por abuso de notación estamos indicando de la misma forma las operaciones de $\mathbb{A}$ y las de $\mathbb{A}[x]$. Es importante que en las definiciones anteriores se distingan bien estas operaciones aun cuando se las indique de la misma manera.

Ejemplo 241.

Si $p = 3 + 2x^2$ y $q = x + (-1)x^3$ entonces

$$p + q = (3 + 0)x^0 + (0 + 1)x^1 + (2 + 0)x^2 + (0 + (-1))x^3 = 3 + x + 2x^2 + (-1)x^3.$$

Para calcular $p.q$ procederemos con más cuidado:

$(p.q)_0 = \sum_{j=0}^{0}(p_j.q_{0-j}) = p_0.q_0 = 3.0 = 0;$

$(p.q)_1 = \sum_{j=0}^{1}(p_j.q_{1-j}) = p_0.q_1 + p_1.q_0 = 3.1 + 0.0 = 3;$

$(p.q)_2 = \sum_{j=0}^{2}(p_j.q_{2-j}) = p_0.q_2 + p_1.q_1 + p_2.q_0 = 3.0 + 0.1 + 2.0 = 0;$

$(p.q)_3 = \sum_{j=0}^{3}(p_j.q_{3-j}) = p_0.q_3 + p_1.q_2 + p_2.q_1 + p_3.q_0 = 3.(-1) + 0.0 + 2.1 + 0.0 = -1;$

$(p.q)_4 = \sum_{j=0}^{4}(p_j.q_{4-j}) = p_0.q_4 + p_1.q_3 + p_2.q_2 + p_3.q_1 + p_4.q_0 = 3.0 + 0.(-1) + 2.0 + 0.1 + 0.0 = 0;$

$(p.q)_5 = \sum_{j=0}^{5}(p_j.q_{5-j}) = p_0.q_5 + p_1.q_4 + p_2.q_3 + p_3.q_2 + p_4.q_1 + p_5.q_0 = 3.0 + 0.0 + 2.(-1) + 0.0 + 0.1 + 0.0 = -2.$

Es fácil ver que para cualquier $i \geq 6$ obtenemos $(p.q)_i = 0$, luego

$$p.q = 3x + (-1)x^3 + (-2)x^5.$$

♢

Observar que si $i > mayor\{gr(p), gr(q)\}$ entonces $(p+q)_i = p_i + q_i = 0+0 = 0$; luego

$$gr(p+q) \leq mayor\{gr(p), gr(q)\}. \tag{7.1}$$

Por otra parte, si $i > gr(p) + gr(q)$ entonces

$$(p.q)_i = \sum_{j=0}^{i} p_j.q_{i-j} = \sum_{j=0}^{gr(p)} p_j.q_{i-j} + \sum_{j=gr(p)+1}^{i} p_j.q_{i-j} =$$

$$= \sum_{j=0}^{gr(p)} p_j.q_{i-j} + \sum_{j=gr(p)+1}^{i} 0.q_{i-j} = \sum_{j=0}^{gr(p)} p_j.q_{i-j} = \sum_{j=0}^{gr(p)} p_j.0 = 0,$$

pues cuando $0 \leq j \leq gr(p)$, tenemos que $i - j > gr(p) + gr(q) - gr(p) = gr(q)$. Resulta que

$$gr(p.q) \leq gr(p) + gr(q). \tag{7.2}$$

Si $\mathbb{A}$ es un anillo de integridad, llamando $n = gr(p)$ y $m = gr(q)$, tenemos que

$$(p.q)_{n+m} = \sum_{j=0}^{n+m} p_j.q_{(n+m)-j} = \sum_{j=0}^{n} p_j.q_{(n+m)-j} + \sum_{j=n+1}^{m} p_j.q_{(n+m)-j} =$$

$$= \sum_{j=0}^{n} p_j.q_{(n+m)-j} + \sum_{j=n+1}^{m} 0.q_{(n+m)-j} = \sum_{j=0}^{n} p_j.q_{(n+m)-j} = \sum_{j=0}^{n} p_j.q_{m+(n-j)} = p_n.p_m \neq 0,$$

porque $p_n \neq 0$ y $q_n \neq 0$ y $\mathbb{A}$ es de integridad. Resulta que

$$\text{si } \mathbb{A} \text{ es de integridad entonces } gr(p.q) = gr(p) + gr(q). \tag{7.3}$$

Los elementos no nulos de $\mathbb{A}$ se identifican con los polinomios de grado 0 de $\mathbb{A}[x]$ haciendo:

$$a \in \mathbb{A} \leftrightarrows ax^0 \in \mathbb{A}[x].$$

Y el elemento nulo de $\mathbb{A}$ se identifica con el polinomio nulo de $\mathbb{A}[x]$ haciendo:

$$0 \in \mathbb{A} \leftrightarrows 0x^0 \in \mathbb{A}[x].$$

Las operaciones suma y producto de $\mathbb{A}$ y de $\mathbb{A}[x]$ son compatibles con esta identifiación en el sentido que dados a y b cualesquiera en $\mathbb{A}$, es lo mismo sumarlos (o multiplicarlos) como elementos de $\mathbb{A}$ que como elementos de $\mathbb{A}[x]$:

$$\begin{array}{cccc} a & b & \text{sumándolos en } \mathbb{A} \text{ obtenemos} & a+b \\ \uparrow\downarrow & \uparrow\downarrow & & \uparrow\downarrow \\ ax^0 & bx^0 & \text{sumándolos en } \mathbb{A}[x] \text{ obtenemos} & (a+b)x^0 \end{array}$$

Teorema 242. *Si* $(\mathbb{A}, +, .)$ *es un anillo conmutativo (con unidad)(de integridad) entonces* $(\mathbb{A}[x], +, .)$ *(aquí* $+$ *y* $.$ *indican las operaciones suma de polinomios y producto de polinomios respectivamente) es un anillo conmutativo (con unidad) (de integridad).*

Demostración: Debemos probar que la suma de polinomios $+$ es una operación asociativa, conmutativa, que admite elemento neutro y que todo $p \in \mathbb{A}[x]$ admite un opuesto según $+$; que el producto de polinomios $.$ es una operación asociativa y conmutativa; y que $.$ es distributiva respecto de $+$.
Sean p, q y h polinomios de $\mathbb{A}[x]$. Para cualquier i vale que

$$(p + (q + h))_i = p_i + (q + h)_i = p_i + (q_i + h_i).$$

Como p_i, q_i y h_i pertenecen a $\mathbb{A}$ y $+$ es asociativa en $\mathbb{A}$, pues se trata de un anillo, entonces

$$p_i + (q_i + h_i) = (p_i + q_i) + h_i = (p + q)_i + h_i = ((p + q) + h)_i.$$

Resulta que para todo i vale que $(p + (q + h))_i = ((p + q) + h)_i$, luego $p + (q + h) = (p + q) + h$, como queríamos probar.
Análogamente se prueba que la suma de polinomios es conmutativa.
Es fácil ver que el polinomio nulo $p = 0$ es neutro para $+$ en $\mathbb{A}[x]$.
Sea $p \in \mathbb{A}[x]$ cualquiera. Para todo i vale que $p_i \in \mathbb{A}$; como A es un anillo, existe $-(p_i) \in A$, opuesto de p_i. Llamamos $-p$ al polinomio de $\mathbb{A}[x]$ tal que $(-p)_i = -(p_i)$ para cada i, resulta que $-p$ es el opuesto de p según la suma de polinomios. Claramente $p + (-p)$ es el polinomio nulo, es decir, $(p + (-p))_i = 0$ para todo i.

Si el anillo $\mathbb{A}$ es con unidad, es decir, existe $1 \in \mathbb{A}$, neutro para .; entonces el polinomio $1x^0$ es neutro para el producto de polinomios.

Probar que el producto de polinomios es asociativo y conmutativo se deja como ejercicio.

Finalmente, si $\mathbb{A}$ es de integridad y p y q son polinomios no nulos entonces, por la relación (7.3), tenemos que $gr(p.q) = gr(p) + gr(q)$; de donde $p.q \neq 0$. Resulta que $\mathbb{A}[x]$ es anillo de integridad. □

Convención: Si p y q son polinomios, para simplificar la notación, en lugar de $p+(-q)$ podemos escribir $p - q$.

Ejercicio 243.

Sea $\mathbb{A}'$ un subconjunto de $\mathbb{A}$. Probar que $\mathbb{A}'[x]$ es un subanillo de $\mathbb{A}[x]$ si y solo si $\mathbb{A}'$ es un subanillo de $\mathbb{A}$. Si llamamos $\mathbb{A}[x]_n = \{p \in \mathbb{A}[x] : p = 0 \vee gr(p) \leq n\}$ entonces $\mathbb{A}[x]_n$ no es necesariamente un subanillo de $A[x]$, pero es un subgrupo de $(\mathbb{A}[x], +)$.♢

Dado p y d polinomios de $\mathbb{A}[x]$, d no nulo, se dice que d **divide a** p o que d **es divisor de** p, o que p **es divisible por** d, o que p **es múltiplo de** d (en $\mathbb{A}[x]$) si existe $q \in \mathbb{A}[x]$ tal que $p = q.d$.

Ejemplo 244.

En $\mathbb{R}[x]$ el polinomio $d = x - 1$ divide al polinomio $p = x^2 - 1$, pues $x^2 - 1 = (x-1).(x+1)$ y $x + 1 \in \mathbb{R}[x]$.

$h = x^3 - x + 1$ no divide a p; si fuera cierto que h divide a p entonces existiría $q \in \mathbb{R}[x]$ tal que $p = h.q$ y en tal caso tendríamos la contradicción: $2 = gr(p) = gr(h) + gr(q) = 3 + gr(q)$. ♢

Usualmente, d divide a p se denota $d \mid p$ y d no divide a p se indica $d \nmid p$.

Cuando $\mathbb{A}$ es un cuerpo conmutativo entonces $\mathbb{A}[x]$ es un anillo conmutativo con unidad íntegro, pero no es un cuerpo. Observar que, ningún polinomio p con grado mayor que 0 admite inverso multiplicativo, pues, si existiera un polinomio $q \in \mathbb{A}[x]$ tal que $p.q = 1$ entonces $gr(p.q) = gr(p) + gr(q) = gr(1) = 0$, contradiciendo que $gr(p) > 0$.

La diferencia que podemos marcar entre $\mathbb{A}[x]$ (cuando $\mathbb{A}$ es un anillo conmutativo con unidad íntegro que no es cuerpo) y $\mathbb{K}[x]$ (cuando $\mathbb{K}$ es un cuerpo) es la existencia de algoritmo de división (Teorema 246).

Por ejemplo, en $\mathbb{Z}[x]$ no se puede hablar un algoritmo de división, pero sí en $\mathbb{Q}[x]$ o

en $\mathbb{R}[x]$ o en $\mathbb{C}[x]$. Veremos ejemplos más adelante.

7.2. Divisibilidad en $\mathbb{K}[x]$

En adelante $(\mathbb{K}, +, .)$ es un cuerpo conmutativo.

Proposición 245. *Sean p y d polinomios de $\mathbb{K}[x]$, no nulos. Si $d \mid p$ entonces $gr(d) \leq gr(p)$.*

Demostración: Si $d \mid p$ entonces existe $q \in \mathbb{K}[x]$ tal que $p = q.d$; luego, como todo cuerpo es anillo de integridad, por la relación (7.3), tenemos que $gr(p) = gr(q.d) = gr(q) + gr(d) \geq gr(d)$, como queríamos probar. □

Teorema 246. *(Algoritmo de la división en $\mathbb{K}[x]$) Dados p y d polinomios cualesquiera de $\mathbb{K}[x]$, d no nulo, existe un único par de polinomios q y r de $\mathbb{K}[x]$ tal que $p = q.d + r \quad y \quad r = 0$ o $gr(r) < gr(d)$. El polinomio q se dice el **cociente** de la división de p por d y el polinomio r se dice el **resto** de la división de p por d.*

Demostración: Si d divide a p, la demostración es trivial considerando $r = 0$.
Si d no divide a p entonces todos los polinomios pertenecientes al conjunto

$$M = \{p - h.d \text{ con } h \in \mathbb{K}[x]\}$$

son no nulos, luego puedo elegir $r \in M$ con grado mínimo, es decir, $r \in M$ y $gr(r)$ es menor o igual que el grado de cualquier polinomio en M.
Como $r \in M$, existe $q \in \mathbb{K}[x]$ tal que $r = p - q.d$, de donde $p = q.d + r$. Es claro que $r \neq 0$, veamos que $gr(r) < gr(d)$.
Supongamos que $m = gr(r) \geq gr(d) = n$. Sea d_n el coeficiente principal de d y r_m el de r. Como $\mathbb{K}$ es un cuerpo puedo considerar $a = \frac{r_m}{d_n} \in \mathbb{K}$.
Sea t el polinomio de $\mathbb{K}[x]$ dado por $t = r - (ax^{m-n}).d$.
Es fácil ver que $gr(t) < gr(r)$; luego, como r es un polinomio de mínimo grado en M, resulta que $t \notin M$, lo cual contradice el hecho que

$$t = r - (ax^{m-n}).d = (p - q.d) - (ax^{m-n}).d = p - (q + (ax^{m-n})).d \ \in M.$$

Veamos ahora que q y r son los únicos polinomios de $\mathbb{K}[x]$ que satisfacen lo pedido.
Efectivamente, supongamos q' y r' son polinomios de $\mathbb{K}[x]$ tales que

$$p = q'.d + r' \quad \text{y} \quad r' = 0 \text{ o } gr(r') < gr(d).$$

Entonces $q.d + r = q'.d + r'$ luego $(q - q').d = r' - r$; si este polinomio es no nulo, tenemos que

$$gr((q - q').d) = gr(q - q') + gr(d) = gr(r' - r) \leq mayor\{gr(r'), gr(r)\} < gr(d);$$

de donde resulta la contradicción $gr(q - q') + gr(d) < gr(d)$.
Concluimos que $(q - q').d = r' - r = 0$, de donde $r = r'$ y $q = q'$ como queríamos probar. □

Dos polinomios p y q de $\mathbb{K}[x]$ se dicen **asociados** si existe $a \in \mathbb{K}$, $a \neq 0$, tal que $p = a.q$.

Ejemplo 247.
En $\mathbb{R}[x]$ los polinomios $p = 2 + 3x + 5x^4$ y $q = 1 + \frac{3}{2}x + \frac{5}{2}x^4$ son asociados pues $q = \frac{1}{2}.p$. También p y $h = \frac{2}{5} + \frac{3}{5}x + x^4$ son asociados.

Ejercicio 248.

1. Probar que la relación $\sim$ definida en $\mathbb{K}[x]$ de la siguiente manera es de equivalencia,

   $p \sim q$ si y sólo si p y q son asociados.

2. Probar que todo polinomio no nulo tiene un único polinomio asociado mónico.
3. Sean p y q asociados. Probar que para cualquier polinomio h vale que $p \mid h$ si y sólo si $q \mid h$; y que $h \mid p$ si y sólo si $h \mid q$.
4. Probar que $p \mid q$ y $q \mid p$ si y sólo si p y q son asociados. ♢

Teorema 249. *(Existencia y unicidad del Máximo Común Divisor) Sean p y q polinomios de $\mathbb{K}[x]$, no ambos nulos. Existe un único polinomio mónico $d \in \mathbb{K}[x]$, tal que:*

i) $d \mid p$ y $d \mid q$; y
ii) para todo $h \in \mathbb{K}[x]$ se verifica que si $h \mid p$ y $h \mid q$ entonces $h \mid d$.

*Observar que como consecuencia de ii) cualquier divisor común de p y de q tiene grado menor o igual que el grado de d, por eso d se llama **máximo común divisor** de p y q; se denota (p, q).*

Demostración: Sea

$$H = \{h \in \mathbb{K}[x] : h \neq 0 \wedge h = m.p + s.q \text{ para algún } m \text{ y } s \text{ en } \mathbb{K}[x]\}.$$

Como p o q es no nulo entonces H es no vacío, luego puedo elegir $d \in H$ mónico de grado mínimo; es decir: d es mónico, $d \in H$ y $gr(d)$ es menor o igual que el grado de cualquier otro polinomio en H. Veamos que d satisface las condiciones del enunciado. Como $d \in H$, existen m y s en $\mathbb{K}[x]$ tales que $d = m.p + s.q$; además, por el algoritmo de la división, existen t y r en $\mathbb{K}[x]$ tales que $p = t.d + r$, y $r = 0$ o $gr(r) < gr(d)$. Si $r \neq 0$ entonces, como $r = p - t.d = p - t.(m.p + s.q) = (1 - t.m).p + (-t.s).q$, tenemos que $r \in H$, lo cual contradice que $gr(r) < gr(d)$ y d con grado mínimo en H. Resulta que $r = 0$, luego $d \mid p$. Análogamente se prueba que $d \mid q$.
Por otra parte, si $h \in \mathbb{K}[x]$ es tal que $h \mid p$ y $h \mid q$ entonces $h \mid m.p + s.q$, luego $h \mid d$; lo cual prueba que $ii)$ se satisface.
La demostración de la unicidad se deja como ejercicio. □

Dados p y q pertenecientes a $\mathbb{K}[x]$ se llama **combinación** (polinómica) de p y q, a todo polinomio h de la forma $h = m.q + s.p$, con m y s polinomios cualesquiera de $\mathbb{K}[x]$. El teorema anterior prueba que el máximo común divisor (p, q) es la combinación no nula, mónica, de menor grado entre todas las combinaciones posibles de p y q. En particular resulta entonces que:

$$\text{existen } m, s \text{ en } \mathbb{K}[x] \text{ tales que } (p, q) = m.p + s.q.$$

El siguiente resultado es la base del **algoritmo de Euclides** que permite el cálculo de (p, q) mediante una secuencia de divisiones. La demostración se omite pues es completamente análoga a la de la Proposición 139.

Proposición 250. *Sean p y q en $\mathbb{K}[x]$ y sea r el resto de la división de p por q. Vale que $(p, q) = (q, r)$.*

Dos polinomios p y q se dicen **coprimos** si $(p, q) = 1$.

Ejercicio 251.

1. Probar que si p y q son asociados entonces para cualquier polinomio h vale que $(p, h) = (q, h)$.
2. Probar que si a y b pertenecen a $\mathbb{K}$ y $a \neq b$ entonces $x - a$ y $x - b$ son polinomios coprimos.

3. Probar que si p y q son coprimos entonces para todo n y m en $\mathbb{N}$ vale que $(p^n, q^m) = 1$.
4. Probar que si p y q son coprimos, $p \mid h$ y $q \mid h$, entonces $p.q \mid h$
5. Probar que si p y q son coprimos y $p \mid q.h$, entonces $p \mid h$.
6. Sean p y q polinomios no nulos. LLamemos h y t a los polinomios cociente de las divisiones de p y de q por (p, q), respectivamente; es decir, $p = h.(p, q)$ y $q = t.(r, s)$. Probar que $(h, t) = 1$.

Teorema 252. *(Existencia y unicidad del Mínimo Común Múltiplo) Sean p y q polinomios de $\mathbb{K}[x]$ ambos no nulos. Existe un único polinomio mónico $m \in \mathbb{K}[x]$, tal que:*

i) $p \mid m$ y $q \mid m$; y

ii) para todo $h \in \mathbb{K}[x]$ se verifica que si $p \mid h$ y $q \mid h$ entonces $m \mid h$.

Observar que como consecuencia de ii) cualquier múltiplo común de p y de q tiene grado mayor o igual que el grado de m, por eso m se llama ***mínimo común múltiplo*** *de p y q; se denota $[p, q]$.*

Demostración: Esta demostración es análoga a la del Teorema 147, daremos solo un esquema de la misma. Sea $H = \{t \in \mathbb{K}[x] : p \mid t \wedge q \mid t\}$. Claramente A es no vacío, por ejemplo $p.q \in H$. Sea m el polinomio de H mónico y con menor grado. Es fácil verificar que m satisface las condiciones del enunciado. □

Ejercicio 253.

1. Sean p y q polinomios de $K[x]$ asociados y no nulos. Probar que para todo polinomio $h \neq 0$ vale que $[p, h] = [q, h]$.
2. Sean p y q en $\mathbb{K}[x]$ no nulos y mónicos. Probar que

$$p.q = (p, q).[p, q].$$

♢

Si p es un polinomio no nulo de $\mathbb{K}[x]$ entonces p es divisible por todo polinomio de grado 0 y también por todo polinomio asociado a p. Estos divisores se llaman **divisores triviales**.

Un polinomio se dice irreducible en $\mathbb{K}[x]$ si tiene grado positivo y sus únicos divisores en $\mathbb{K}[x]$ son los triviales. En otras palabras, $p \in \mathbb{K}[x]$ con $gr(p) > 0$ es **irreducible** en $\mathbb{K}[x]$ si y sólo si

$$p = q.h \text{ con } q \text{ y } h \text{ en } \mathbb{K}[x] \text{ implica } gr(q) = 0 \text{ o } gr(h) = 0.$$

En forma equivalente se puede pensar que un polinomio $p \in \mathbb{K}[x]$ con grado positivo es **reducible** (no irreducible) si se puede escribir como producto de dos polinomios de $\mathbb{K}[x]$ cada uno de ellos con grado mayor o igual que uno.
Observar que todo polinomio de grado uno es irreducible.
Un polinomio se dice **primo** si es irreducible y mónico.
Ejercicio 254.

1. Probar que si p es irreducible y q es asociado con p entonces q es irreducible.
2. Si p es irreducible y $p \nmid q$ entonces $(p, q) = 1$.
3. Si p es irreducible y $p \mid q.h$, entonces $p \mid q$ o $p \mid h$. ♢

Veremos a continuación que el anillo de polinomios con coeficientes en un cuerpo es, al igual que el anillo de los números entero, un **dominio de factorización única**, es decir, todo elemento del anillo se descompone de un única manera como producto de elementos primos.

Proposición 255. *Si $p \in \mathbb{K}[x]$ tiene grado positivo entonces existe $q \in \mathbb{K}[x]$ primo tal que q divide a p.*

Demostración: Sin pérdida de generalidad podemos suponer que p es mónico. Haremos inducción en $gr(p)$. Si $gr(p) = 1$ entonces p es primo y la proposición es verdadera considerando $q = p$. Si $gr(p) > 1$ y p es irreducible, nuevamente la proposición es trivialmente verdadera considerando $q = p$. Si p no es irreducible existen polinomios h y t en $\mathbb{K}[x]$ tales que $gr(h) > 0$, $gr(t) > 0$ y $p = h.t$, luego $gr(h) < gr(p)$. Resulta, por hipótesis inductiva, que existe q primo tal que q divide a h. Así tenemos que q divide a p, como queríamos probar. □

Teorema 256. *(Teorema Fundamental de la Aritmética en $\mathbb{K}[x]$) Sea $p \in \mathbb{K}[x]$ con grado positivo. Existen polinomios primos $p_1, p_2, ..., p_k \in$ en $K[x]$ y $a \in \mathbb{K}$ tales que:*

$$p = a.p_1.p_2...p_k.$$

Esta escritura que se llama ***descomposición de*** p ***en factores primos*** *(o* ***factorización de*** p ***en primos****) es única salvo el orden en que se consideren los factores.*

Demostración: Nuevamente consideramos p mónico y hacemos inducción en $gr(p)$. Si $gr(p) = 1$, la demostración es trivial, pues, en tal caso, p es primo. Si $gr(p) > 1$ y p es primo, la demostración es trivial. Ahora asumamos que p no es primo. Por la Proposición 255 existe p_0 primo que divide a p, luego $p = p_0.h$. Como p no es primo resulta que $gr(h) > 0$, entonces, por hipótesis inductiva, h se factoriza en primos p_1,...,p_k. Resulta que $p = p_0.p_1....p_k$ como queríamos probar.
La demostración de la unicidad de escritura se deja como ejercicio. □
Para analizar cuales son los polinomios de $\mathbb{R}[x]$ y de $\mathbb{C}[x]$ que son primos utilizaremos el concepto de raíz de un polinomio.

7.3. Raíces de un polinomio

En lo que sigue, con $\mathbb{A}$ indicaremos un anillo conmutativo y con $\mathbb{K}$ un cuerpo conmutativo.
Sea $p = p_0 + p_1x^1 + ... + p_nx^n$ un polinomio de $\mathbb{A}[x]$ y sea $a \in \mathbb{A}$. Llamamos **valor de** p **en** a al elemento de $\mathbb{A}$ que se denota $p(a)$ y que se obtiene haciendo

$$p(a) = p_0 + p_1.a^1 + ... + p_n.a^n;$$

aquí + y . representan las operaciones de $\mathbb{A}$.

Ejercicio 257.

1. Si p y q pertenecen a $\mathbb{A}[x]$ y $a \in \mathbb{A}$ entonces $(p+q)(a) = p(a) + q(a)$ (el primer + es la operación de $\mathbb{A}[x]$ y el segundo + es la operación de $\mathbb{A}$).
2. Si p y q pertenecen a $\mathbb{A}[x]$ y $a \in \mathbb{A}$ entonces $(p.q)(a) = p(a).q(a)$ (el primer . es la operación de $\mathbb{A}[x]$ y el segundo . es la operación de $\mathbb{A}$). ♢

Un elemento $a \in \mathbb{A}$ se dice una **raíz del polinomio** $p \in \mathbb{A}[x]$ si $p(a) = 0$.

Teorema 258. *(Teorema de Gauss) Sea p un polinomio con coeficientes en* $\mathbb{Z}$ *y sea* $\frac{a}{b} \in \mathbb{Q}$ *con* a *y* b *enteros coprimos no nulos. Si* $p(\frac{a}{b}) = 0$ *entonces* $a \mid p_0$ *y* $b \mid p_n$.

Demostración: Como $p(\frac{a}{b}) = p_0 + p_1.(\frac{a}{b})^1 + ... + p_n.(\frac{a}{b})^n = 0$, multiplicando por b^n a ambos lados de la igualdad tenemos que $p_0.b^n + p_1.a.b^{n-1} + ... + p_n.a^n.b^{n-n} = 0$.

Luego $b.(p_0.b^{n-1} + p_1.a.b^{n-2} + ... + p_{n-1}.a^{n-1}.b^{n-(n-1)-1)}) + p_n.a^n = 0$, de donde b divide a $p_n.a^n$. Como por hipótesis b y a son coprimos, resulta que b divide a p_n.
Análogamente, haciendo

$$p_0.b^n + p_1.a.b^{n-1} + ... + p_n.a^n.b^{n-n} = p_0.b^n + a.(p_1.b^{n-1} + ... + p_n.a^{n-1}.b^{n-n}) = 0,$$

resulta que a divide a p_0. □

Ejemplo 259.

Nos preguntamos si existe algún número racional $\frac{a}{b}$ que sea raíz del polinomio $p = x^5 - 4x^3 + 2x + 5$. Como todos los coeficientes de p son enteros, por el Teorema de Gauss sabemos que si $\frac{a}{b}$ es raíz de p entonces a divide 5 y b divide a 1. Luego debe ser $a \in \{1, -1, 5, -5\}$ y $b \in \{1, -1\}$. Resulta que las únicas posibles raíces racionales de p son 1, -1, 5 y -5. Verificando en forma directa tenemos que $p(1) = 4$, $p(-1) = 6$, $p(5) = 2640$ y $p(-5) = 2630$; luego p no tiene raíces racionales.

Teorema 260. *(Teorema del resto) Sea $p \in \mathbb{K}[x]$ y $a \in \mathbb{K}$. El resto de dividir a p por $x - a$ es igual a $p(a)$.*

Demostración: Sean q y r en $\mathbb{K}[x]$ tales que

$$p = q.(x - a) + r \text{ con } r = 0 \text{ o } 0 \leq gr(r) < gr(x - a).$$

Como $gr(x-a) = 1$ tenemos que $r \in \mathbb{K}$. Luego, $p(a) = q(a).(a-a)+r = q(a).0+r = 0 + r = r$, como queríamos probar. □

Corolario 261. *Sea $p \in \mathbb{K}[x]$ y $a \in \mathbb{K}$; a es raíz de p si y sólo si $(x - a)$ divide a p.*

Corolario 262. *Sea $p \in \mathbb{K}[x]$ con $gr(p) > 1$. Si p tiene alguna raíz en $\mathbb{K}$ entonces p es reducible en $\mathbb{K}[x]$.*

Observar que los resultados anteriores dicen que si $a \in \mathbb{K}$ es una raíz de $p \in \mathbb{K}[x]$ entonces $(x - a)$ es uno de los factores primos que aparecen en la descomposición de p. La cantidad de veces que aparece este factor es lo que a continuación se define como multiplicidad.

Si a es una raíz de p, se llama **grado de multiplicidad de a como raíz de p**, al mayor natural m tal que $(x - a)^m \mid p$. También se suele decir que a **es una raíz de multiplicidad m de p**. La multiplicidad de a como raíz de p se indica $m_p(a)$ o m_p. Es claro que $m_p(a) \leq gr(p)$.

Proposición 263. *Sea $p \in \mathbb{K}[x]$ y $a_1, a_2, ..., a_k$ elementos de $\mathbb{K}$ distintos entre sí, raíces de p con multiplicidad $m_1, m_2, ..., m_k$, respectivamente. Se satisface que*

$$(x - a_1)^{m_1}.(x - a_2)^{m_2}...(x - a_k)^{m_k} \text{ divide a } p.$$

Demostración: Por definición de multiplicidad tenemos que existen polinomios h_1 y h_2 tales que $p = (x - a_1)^{m_1}.h_1$ y $p = (x - a_2)^{m_2}.h_2$, luego

$$(x - a_1)^{m_1}.h_1 = (x - a_2)^{m_2}.h_2. \quad (7.4)$$

Como $a_1 \neq a_2$, $x - a_1$ y $x - a_2$ son coprimos, luego $(x - a_1)^{m_1}$ y $(x - a_2)^{m_2}$ son coprimos. Resulta de (7.4) que $(x - a_2)^{m_2}$ divide a h_1, luego existe un polinomio h_3 tal que $p = (x - a_1)^{m_1}.h_1 = (x - a_1)^{m_1}.(x - a_2)^{m_2}.h_3$

Repitiendo este procedimiento se completa la demostración. □

Ejemplo 264.

El polinomio $p = (x-2)^3.(x+4)^2.(x-\sqrt{2})$ admite 3 **raíces distintas** las cuales son: 2, -4 y $\sqrt{2}$. La multiplicidad de 2 es 3, la multiplicidad de -4 es 2 y la multiplicidad de $\sqrt{2}$ es 1. También se dice que p admite 6 **raíces contadas con sus multiplicidades**, pues 6=3+2+1. ♢

Corolario 265. *Un polinomio $p \in \mathbb{K}[x]$ con grado n tiene a lo sumo n raíces en $\mathbb{K}$ contadas con sus multiplicidades.*

Ejemplo 266.

Dada la ecuación $x^{56} - 27x^{14} + 4x^8 + \sqrt{2}x - \frac{\pi}{5} = 0$, no se puede decir a simple vista si existen números reales que satisfaga esta ecuación; pero con seguridad se puede afirmar que a lo sumo hay 56 números reales que la satisfacen.

Así mismo, por ejemplo, se puede afirmar que no existe un polinomio de grado 4 en $\mathbb{C}[x]$ cuyas raíces sean 1, 2, 3, 4 y 5. ♢

Proposición 267. *Sean p y q en $\mathbb{K}[x]$ tales que p divide a q. Si $a \in \mathbb{K}$ es raíz de p entonces a también es raíz de q y, además, $m_p(a) \leq m_q(a)$.*

Demostración: Como $p \mid q$ entonces existe $h \in \mathbb{K}[x]$ tal que $q = p.h$. Luego, $q(a) = p(a).h(a) = 0.h(a) = 0$. Por otra parte, si $m = m_p(a)$ entonces $(x - a)^m \mid p$; y como $p \mid q$ resulta $(x - a)^m \mid q$. Concluimos que $m \leq m_q(a)$, como queríamos probar. □

Como $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ entonces $\mathbb{Z}[x] \subset \mathbb{Q}[x] \subset \mathbb{R}[x] \subset \mathbb{C}[x]$. Luego, cuando decimos que un polinomio perteneciente a alguno de estos conjuntos tiene o no tiene raíces debemos tener cuidado de indicar en dónde.

Ejemplo 268.

Si estoy trabajando en $\mathbb{Z}[x]$, debo decir que el polinomio $p = 2x - 3$ no tiene raíces. En cambio, en $\mathbb{Q}[x]$ sí tiene raíz, pues p admite la raíz $\frac{3}{2} \in \mathbb{Q}$.

El polinomio $x^4 - 2$ no admite raíces en $\mathbb{Q}$, admite dos raíces en $\mathbb{R}$ que son $\sqrt[4]{2}$ y $-\sqrt[4]{2}$; y admite cuatro raíces en $\mathbb{C}$: $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $\sqrt[4]{2}i$, y $-\sqrt[4]{2}i$.

El polinomio $x^2 + 1$ no admite raíces en $\mathbb{R}$, pero tiene dos raíces en $\mathbb{C}$: i y $-i$.

¿Existe algún polinomio de $\mathbb{C}[x]$ que no admita raíces en $\mathbb{C}$? ♢

Un cuerpo $\mathbb{K}$ se dice **algebraicamente cerrado** si todo polinomio de $\mathbb{K}[x]$ con grado mayor que 0 tiene al menos una raíz en $\mathbb{K}$. Como vimos en el ejemplo anterior $\mathbb{Q}$ no es algebraicamente cerrado y $\mathbb{R}$ no es algebraicamente cerrado. El siguiente teorema, cuya demostración omitiremos, establece que el cuerpo de los números complejos sí es algebraicamente cerrado.

Teorema 269. *(Teorema Fundamental del Algebra) El cuerpo $\mathbb{C}$ de los números complejos es algebraicamente cerrado. Es decir,*

$$\textit{si } p \in \mathbb{C}[x] \textit{ y } gr(p) > 0 \textit{ entonces existe } z \in \mathbb{C} \textit{ tal que } p(z) = 0.$$

Corolario 270. *Si $p \in \mathbb{C}[x]$ y $gr(p) = n > 0$, entonces p admite exactamente n raíces contadas con sus respectivas multiplicidades.*

Demostración: Sean z_1, z_2,...,z_k todas las distintas raíces de p con multiplicidades m_1, m_2,...,m_k respectivamente. Supongamos que $m_1+m_2+...+m_k < n$. Por lo probado en la Proposición 263, existe $h \in \mathbb{C}[x]$ tal que $p = (x-z_1)^{m_1}.(x-z_2)^{m_2}.....(x-z_k)^{m_k}.h$. Luego, $n = gr(p) = m_1 + m_2 + ... + m_k + gr(h) < n + gr(h)$, entonces $gr(h) > 0$ y así, por el Teorema 269, h admite una raíz $z \in \mathbb{C}$. Si $z = z_i$ para algún i, se contradice que m_i es la multiplicidad de z_i; y si $z \neq z_i$ para todo i, se contradice que z_1, z_2,...,z_k son todas las raíces de p. Resulta que $m_1 + m_2 + ... + m_k = n$. □

Corolario 271. *Los únicos polinomios primos de $\mathbb{C}[x]$ son los mónicos de grado 1, es decir, los de la forma $x - z_0$ con $z_0 \in \mathbb{C}$ cualquiera.*

Podemos concluir que la factorización en primos en $\mathbb{C}[x]$ de cualquier polinomio $p \in \mathbb{C}[x]$ es de la forma

$$p = a.(x - z_1)^{m_1}.(x - z_2)^{m_2}.....(x - z_k)^{m_k}$$

donde $a \in \mathbb{C}$ es el coeficiente principal de p y z_1, z_2,...,z_k son todas las raíces de p con multiplicidades m_1, m_2...m_k respectivamente.
A diferencia de lo que ocurren en $\mathbb{C}[x]$, en $\mathbb{R}[x]$ los polinomios de grado uno no son los únicos irreducibles.

Ejemplo 272.
$p = x^2 + 1$ es irreducible en $\mathbb{R}[x]$, además, como es mónico podemos decir que es primo en $\mathbb{R}[x]$. ¿Será que todos los polinomios de $\mathbb{R}[x]$ con grado 2 son irreducibles? Claramente, no; por ejemplo, $q = x^2 + 2x + 1$ es reducible pues $q = (x + 1)^2$. En lo que sigue analizaremos esta cuestión. ♢

Proposición 273. *Si $z \in \mathbb{C}$ es raíz de $p \in \mathbb{R}[x]$ entonces el conjugado de z también es raíz de p. Más aún, $m_p(z) = m_p(\overline{z})$.*

Demostración: Sea $p = \sum_{i=0}^{n} p_i x^i$ con $p_i \in \mathbb{R}$ para todo i. Como z es raíz tenemos que $p(z) = \sum_{i=0}^{n} p_i z^i = 0$; y como $p_i \in \mathbb{R}$ entonces $p_i = \overline{p_i}$ para todo i. Resulta de lo anterior y de las propiedades de la conjungación que

$$p(\overline{z}) = \sum_{i=0}^{n} p_i \overline{z}^i = \sum_{i=0}^{n} \overline{p_i}\,\overline{z^i} = \sum_{i=0}^{n} \overline{p_i z^i} = \overline{\sum_{i=0}^{n} p_i z^i} = \overline{0} = 0.$$

Ahora llamemos $m = m_p(z)$ y $s = m_p(\overline{z})$; sin pérdida de generalidad podemos suponer $m < s$ y $z \neq \overline{z}$, en otro caso el resultado es trivial. Por Teorema 263, existe $h \in \mathbb{C}[x]$ tal que $p = (x - z)^m.(x - \overline{z})^s.h$; con $h(z) \neq 0$ y $h(\overline{z}) \neq 0$. Observar que $d = (x - z)^m.(x - \overline{z})^m \in \mathbb{R}[x]$, luego por el algoritmo de la división existen q y r en $\mathbb{R}[x]$ tales que $p = d.q + r$ con $r = 0$ o $0 \leq gr(r) < gr(d)$.
Con esto tenemos que,

$$p = (x - z)^m.(x - \overline{z})^s.h = (x - z)^m.(x - \overline{z})^m.(x - \overline{z})^{s-m}.h = d.(x - \overline{z})^{s-m}.h = q.d + r.$$

De las dos últimas igualdades resulta que $r = d.((x - \overline{z})^{s-m}.h - q)$, lo cual contradice $gr(r) < gr(d)$; por lo tanto debe ser $r = 0$ y así $(x - \overline{z})^{s-m}.h - q = 0$, es decir

$$q = (x - \overline{z})^{s-m}.h.$$

Esto es un absurdo, pues $q \in \mathbb{R}[x]$, $\overline{z}$ es raíz de q, pero z no es raíz de q. □

Corolario 274. *Si $p \in \mathbb{R}[x]$ con $gr(p)$ impar entonces p tiene una raíz real. En particular si $gr(p) \geq 3$ y es impar entonces p es reducible en $\mathbb{R}[x]$.*

Ejemplo 275.

Que un polinomio $p \in \mathbb{R}[x]$ no tenga raíces en $\mathbb{R}$ no implica que p sea irreducible en $\mathbb{R}[x]$. Observar que el polinomio $p = x^4 + 2x^2 + 1 = (x^2+1)^2 = (x-i)^2.(x+i)^2$ no tiene raíces reales, pero se factoriza en $\mathbb{R}[x]$ porque $p = (x^2+1).(x^2+1)$. Resulta que p es reducible en $\mathbb{R}[x]$. ♢

Proposición 276. *Los polinomios irreducibles de $\mathbb{R}[x]$ son los polinomios de grado 1 y los polinomios de grado 2 que no admiten raíces reales. En otras palabras, $p \in \mathbb{R}[x]$ es primo si y sólo si*

$p = x - a$ *para algún* $a \in \mathbb{R}$ *o*

$p = (x - z_0).(x - \overline{z_0}) = x^2 + 2.Re(z_0) + \mid z_0 \mid^2$ *para algún* $z_0 \in \mathbb{C} - \mathbb{R}$.

Demostración: Es claro que los polinomios de grado uno y los polinomios de grado dos sin raíces reales son irreducibles; veamos que son los únicos irreducibles de $\mathbb{R}[x]$. Sea $p \in \mathbb{R}[x]$ irreducible. Si $gr(p) \geq 2$ y p tiene alguna raíz real, entonces p es reducible por Corolario 262.

Si $gr(p) > 2$ y p no tiene raíces reales, entonces, por la Proposición 273, sus raíces deben ser $z_1, \overline{z_1}, ..., z_k, \overline{z_k}$ pertenecientes a $\mathbb{C} - \mathbb{R}$ con multimplicidades $m_1, ..., m_k$ respectivamente; es decir,

$$p = (x - z_1)^{m_1}.(x - \overline{z_1})^{m_1}...(x - z_k)^{m_k}.(x - \overline{z_k})^{m_k} =$$

$$= ((x - z_1).(x - \overline{z_1}))^{m_1}...((x - z_k).(x - \overline{z_k}))^{m_k}.$$

Como $(x - z_i).(x - \overline{z_i}) \in \mathbb{R}[x]$ para todo i, resulta que p es reducible en $\mathbb{R}[x]$.

Concluimos que $gr(p) = 1$, o $gr(p) = 2$ y p no tiene raíces reales. □

Observar que un polinomio de $\mathbb{R}[x]$ con grado 2 y sin raíces reales debe ser de la forma $p = x^2 - (2a)x + (a^2 + b^2)$ con a y b pertenecientes a $\mathbb{R}$ y $b \neq 0$.

7.4. Polinomio derivado

En lo que sigue consideramos $\mathbb{K} = \mathbb{Q}$ o $\mathbb{K} = \mathbb{R}$ o $\mathbb{K} = \mathbb{C}$. En general los resultados que daremos a continuación valen cuando $\mathbb{K}$ es un cuerpo con **característica** 0; esto

significa $1 + 1 + 1 + ... + 1 \neq 0$ cualquiera sea la cantidad de unos que sume. Por ejemplo, $\mathbb{Z}_3$, $\mathbb{Z}_5$ y en general $\mathbb{Z}_p$ con p primo no son cuerpos con caracterísitca 0.

Sea $p = p_0 + p_1x^1 + ... + p_nx^n$ un polinomio cualquiera de $\mathbb{K}[x]$. Se llama **polinomio derivado de** p y se denota p' al polinomio de $\mathbb{K}[x]$ dado por

$$p' = p_1 + (2p_2)x^1 + ... + (np_n)x^{n-1}.$$

Observación: es claro que el polinomio derivado que se obtiene a partir de esta definición es exactamente el mismo que se obtiene analíticamente cuando se considera el límite del cociente incremental de funciones polinómicas. Sin embargo para obtener los resultados algebraicos que veremos no es necesario introducir tales conceptos.

Ejemplo 277.

Si $p = 4x^5 - 5x^3 + x - 8$ entonces $p' = 20x^4 - 15x^2 + 1$. ♢

Ejercicio 278.

Probar que $(p + q)' = p' + q'$ y $(p.q)' = p'.q + p.q'$. ♢

Proposición 279. *Sea* $p \in \mathbb{K}[x]$ *y* $a \in \mathbb{K}$ *raíz de* p. *Vale que* $m_p(a) > 1$ *si y sólo si* a *es raíz de* p'. *Además, en tal caso,* $m_{p'}(a) = m_p(a) - 1$.

Demostración: Sea $m = m_p(a)$, luego $p = (x - a)^m.h$ con $h \in \mathbb{K}[x]$ y $h(a) \neq 0$.

Si $m = 1$ entonces $p' = h + (x - a).h'$; luego

$$p'(a) = h(a) + (a - a).h'(a) = h(a) \neq 0.$$

Si $m > 1$ entonces $p' = m.(x - a)^{m-1}.h + (x - a)^m.h'$; de donde

$$p'(a) = m.(a - a)^{m-1}.h + (a - a)^m.h' = 0.$$

Además, como $p' = (x-a)^{m-1}(m.h+(x-a).h')$ y $(m.h+(x-a).h')(a) = m.h(a) \neq 0$, resulta que $m_{p'}(a) = m - 1$, como queríamos probar. □

Ejercicio 280.

Sea $p \in \mathbb{K}[x]$. Llamamos $\frac{p}{(p,p')}$ al polinomio de $\mathbb{K}[x]$ cociente de dividir p por (p, p'). Probar que $\frac{p}{(p,p')}$ tiene exactamente las mismas raíces que p pero todas ellas simples, es decir, con multiplicidad 1. ♢

La proposición anterior se puede generalizar utilizando derivadas sucesivas.

Sea $p \in \mathbb{K}[x]$ y $k \in \mathbb{N}_0$. Se define en forma recursiva el **polinomio derivado** k**-ésimo** de p, que se denota $p^{(k)}$, de la siguiente manera:

$$p^{(k)} = \begin{cases} p & \text{si } k = 0 \\ p' & \text{si } k = 1 \\ (p^{(k-1)})' & \text{si } k > 1 \end{cases}$$

También suele notarse: $p^{(2)} = p''$ y $p^{(3)} = p'''$.

Observar que para todo k se verifica que $(p^{(k)})' = (p')^{(k)}$.

Proposición **281.** *Sea $p \in \mathbb{K}[x]$, $a \in \mathbb{K}$ raíz de p y $n \in \mathbb{N}$, $n \geq 2$. Vale que $m_p(a) = n$ si y sólo si*

$$p'(a) = p''(a) = ... = p^{(m-1)}(a) = 0 \text{ y } p^{(m)}(a) \neq 0.$$

Demostración: Haremos inducción sobre n.

El enunciado es verdadero para $n = 2$ por la Proposición 279.

Sea $n > 2$, a raíz de p y $m_p(a) = n$.

Por la Proposición 279, a es raíz de p' con multiplicidad $n-1$, entonces, por hipótesis inductiva, tenemos que

$$(p')'(a) = (p')''(a) = ... = (p')^{(n-2)}(a) = 0 \text{ y } (p')^{(n-1)}(a) \neq 0;$$

luego

$$p'(a) = p''(a) = p'''(a) = ... = p^{(n-1)}(a) = 0 \text{ y } p^{(n)}(a) \neq 0.$$

Recíporcamente, si

$$p'(a) = p''(a) = p'''(a) = ... = p^{(n-1)}(a) = 0 \text{ y } p^{(n)}(a) \neq 0,$$

entonces a es raíz de p' y

$$(p')'(a) = (p')''(a) = ... = (p')^{(n-2)}(a) = 0 \text{ y } (p')^{(n-1)}(a) \neq 0;$$

Como $n-1 \geq 2$, por hipótesis inductiva tenemos que a es raíz de p' con multiplicidad $n-1$. Como además, por hipótesis, a es raíz de p, resulta que a es raíz de p con multiplicidad n, como queríamos probar. □

Ejercicio 282.

Probar que si $p \in \mathbb{K}[x]$, $n = gr(p)$ y $a \in \mathbb{K}$, entonces

$$p = \sum_{k=0}^{n} \frac{p^{(k)}(a)}{k!}(x-a)^k.$$

Esta forma de escribir el polinomio p se dice **desarrollo de Taylor** de p en potencias de $x - a$. ◇

Ejemplo 283.

Si queremos expresar un polinomio en potencias de de $x - a$ para algún valor fijo de a, podemos hacer uso de la fórmula de Taylor. Veamos como desarrollar el polinomio $p = 3x^2 - x + 1$ en potencias de $x - 10$. De acuerdo a la Fórmula de Taylor

$$p = p(10) + p'(10)(x - 10) + \frac{p''(10)}{2!}(x - 10)^2.$$

Calculando tenemos que,

$$\begin{array}{rcccrcl} p & = & 3x^2 - x + 1 & \text{luego} & p(10) & = & 291 \\ p' & = & 6x - 1 & \text{luego} & p'(10) & = & 59 \\ p'' & = & 6 & \text{luego} & p''(10) & = & 6 \end{array}$$

Resulta que

$$p = 291 + 59(x - 10) + \frac{6}{2}(x - 10)^2.$$



AUTORA

Liliana Alcón, obtuvo el título de Licenciada en Matemática en la Facultad de Ciencias Exactas y Naturales de la Universidad Nacional de Buenos Aires y el título de Doctora en Ciencias Exactas con orientación Matemática en la Facultad de Ciencias Exactas de la Universidad Nacional de La Plata. Es Profesora Adjunta y desarrolla tareas docentes y de investigación en el área de Matemática Discreta en el Departamento de Matemática de esta última Facultad.